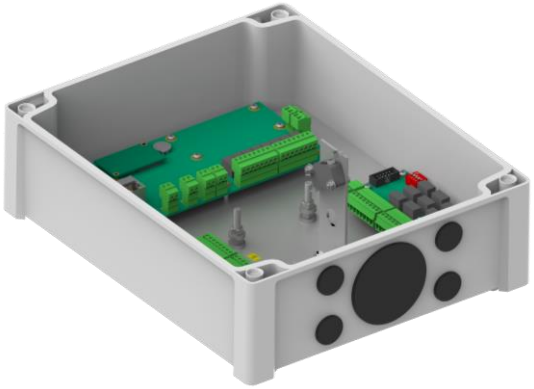
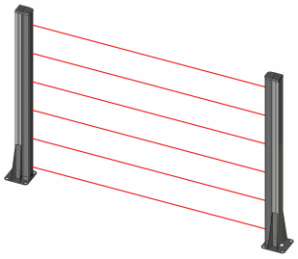
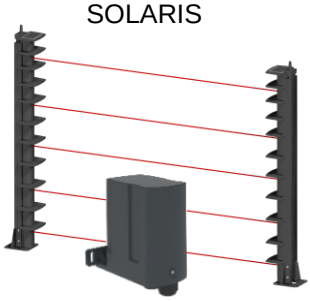
MAXIBUS UNIVERSEL



MAXIRIS 3000



SOLARIS



COORDINATEUR CONNECT

G-FENCE 3000

PIRAMID CONNECT

G-FENCE 2400

MODULE DEPORTE 8 ENTREES

FR **CONCENTRATEUR MAXIBUS UNIVERSEL**
Notice d'installation - Pages 1-41

EN **HUB MAXIBUS UNIVERSAL**
Installation instructions - Pages 42-82

1, rue du Dauphiné – CS 90323 – 69517 VAULX-EN-VELIN CEDEX – FRANCE
Tél. : +33(0)4.78.03.06.10 - Fax : +33(0)4.78.68.24.61 **Site web :** www.sorhea.com **Email :** commercial@sorhea.fr

NT397 / V2.1 / 10.21

SOMMAIRE

1 INTRODUCTION

Le concentrateur MAXIBUS UNIVERSEL permet de centraliser les informations d'alarmes des produits SORHEA.

Il se compose d'une **carte mère** gérant 4 ports COM, 8 contacts d'alarmes. Des contacts d'alarmes supplémentaires sont disponibles à l'aide de **cartes extension 8 relais**.

Nota : le concentrateur MAXIBUS UNIVERSEL s'installe uniquement en intérieur.

1.1 Principales fonctionnalités

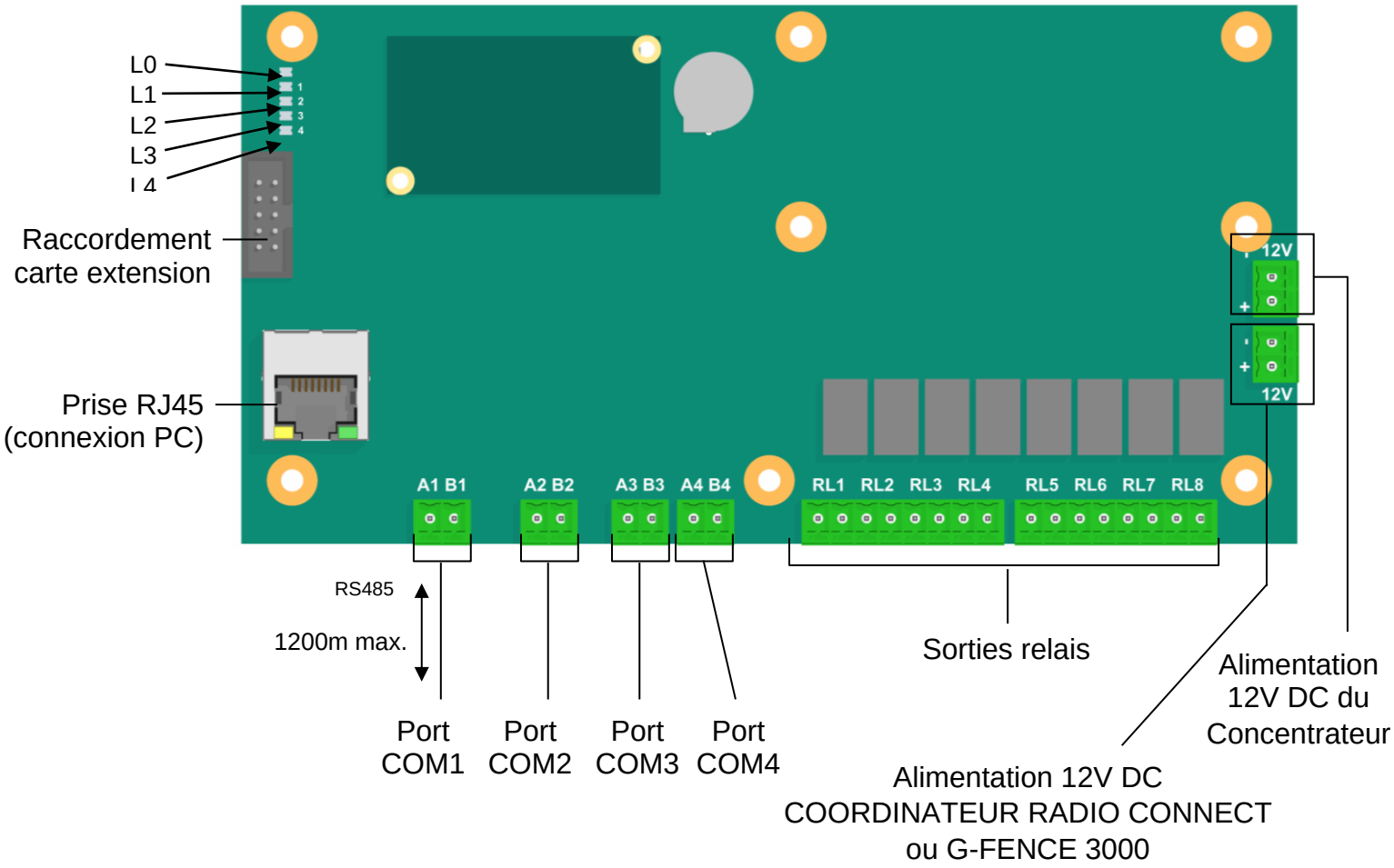
- Centralisation des informations d'alarmes de l'ensemble des détecteurs raccordés sur le réseau.
- Configuration automatique du réseau :
  - Détection des détecteurs raccordés sur le réseau
  - Détection du nombre de contacts disponibles
- Diagnostic de chacun des détecteurs.

1.2 Options

- Carte extension 8 relais (maximum 16 cartes extensions)

2 DESCRIPTION

2.1 Carte concentrateur MAXIBUS UNIVERSEL

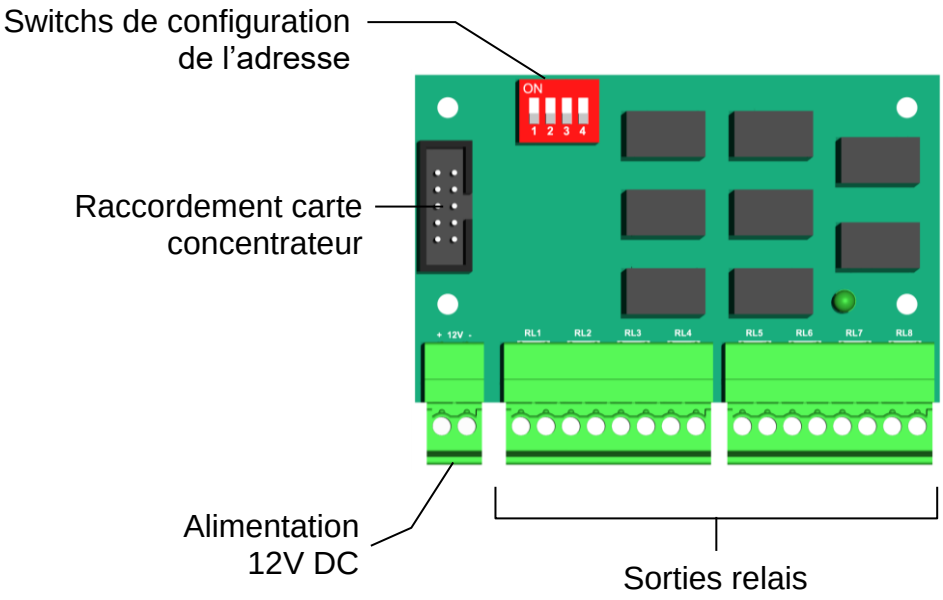


Etats des différents voyants :

Etats du voyant L0 (vert)	Allumé	Démarré
	Eteint	Hors tension / démarrage en cours
Etats du voyant L1 (rouge)	Eteint	Port COM1 du concentrateur non configuré
	Allumé	Port COM1 du concentrateur configuré
	Clignotant	Port COM1 du concentrateur en cours de scrutation
Etats du voyant L2 (rouge)	Eteint	Port COM2 du concentrateur non configuré
	Allumé	Port COM2 du concentrateur configuré
	Clignotant	Port COM2 du concentrateur en cours de scrutation
Etats du voyant L3 (rouge)	Eteint	Port COM3 du concentrateur non configuré
	Allumé	Port COM3 du concentrateur configuré
	Clignotant	Port COM3 du concentrateur en cours de scrutation
Etats du voyant L4 (rouge)	Eteint	Port COM4 du concentrateur non configuré
	Allumé	Port COM4 du concentrateur configuré
	Clignotant	Port COM4 du concentrateur en cours de scrutation

Nota : Chaque port COM peut gérer jusqu'à 32 produits réseau connectés.
Chaque produit connecté possède une adresse réseau unique de 1 à 127 par port COM.

2.2 Carte extension 8 relais

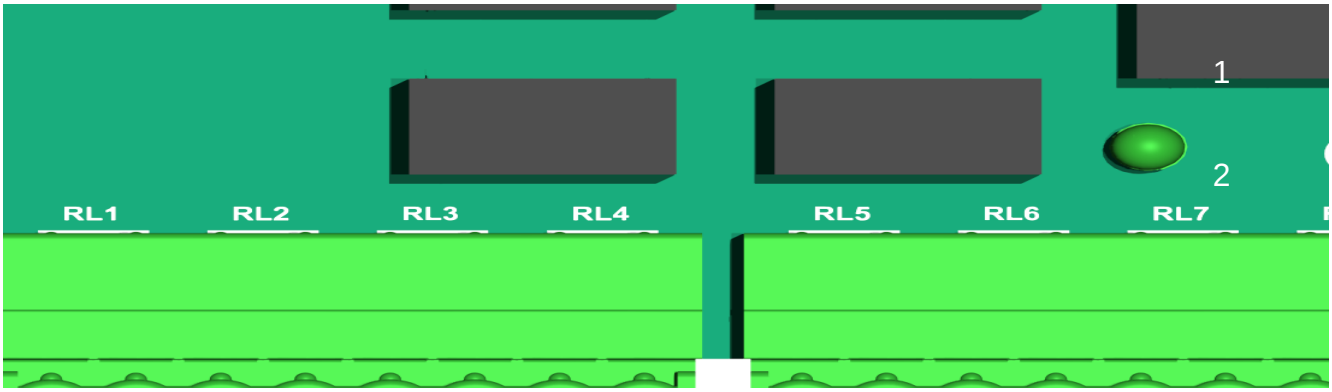


Le concentrateur MAXIBUS UNIVERSEL peut gérer un maximum de 16 cartes extension 8 relais. Chaque carte extension est repérée par une adresse fixée à l'aide des switchs de configuration comme suit :

Position des switchs	Adresse	Position des switchs	Adresse
	1 (OFF OFF OFF OFF)		9 (ON OFF OFF OFF)
	2 (OFF OFF OFF ON)		10 (ON OFF OFF ON)
	3 (OFF OFF ON OFF)		11 (ON OFF ON OFF)
	4 (OFF OFF ON ON)		12 (ON OFF ON ON)
	5 (OFF ON OFF OFF)		13 (ON ON OFF OFF)
	6 (OFF ON OFF ON)		14 (ON ON OFF ON)
	7 (OFF ON ON OFF)		15 (ON ON ON OFF)
	8 (OFF ON ON ON)		16 (ON ON ON ON)

3 RACCORDEMENTS

3.1 Raccordement du concentrateur MAXIBUS UNIVERSEL

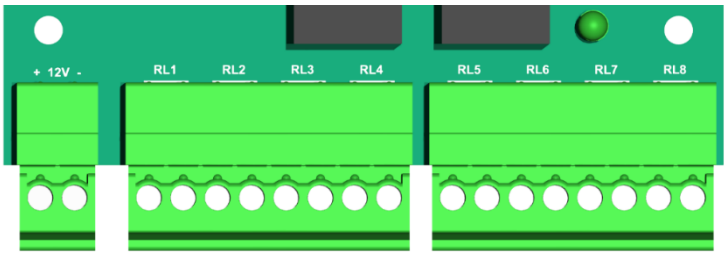


A1	Borne A sortie bus RS485 COM1	RL4		Contacts relais 4
B1	Borne B sortie bus RS485 COM1	RL4		
A2	Borne A sortie bus RS485 COM2	RL5		Contacts relais 5
B2	Borne B sortie bus RS485 COM2	RL5		
A3	Borne A sortie bus RS485 COM3	RL6		Contacts relais 6
B3	Borne B sortie bus RS485 COM3	RL6		
A4	Borne A sortie bus RS485 COM4	RL7		Contacts relais 7
B4	Borne B sortie bus RS485 COM4	RL7		
RL1	Contacts relais 1	RL8		Contacts relais 8
RL1		RL8		
RL2	Contacts relais 2	1	-	Entrée alimentation 0V
RL2			+	Entrée alimentation +12V DC
RL3	Contacts relais 3	2	-	Sortie 0V port COM
RL3			+	Sortie +12V DC port COM

Les contacts des relais sont fermés hors alarme. Ils sont ouverts si alarme ou si affectés ou si concentrateur hors tension. (Sécurité positive)

L'alimentation 12V du concentrateur MAXIBUS UNIVERSEL doit être équipée d'un fusible 2A rapide.
Elle doit être raccordée à la terre de protection.

3.2 Raccordement carte extension 8 relais

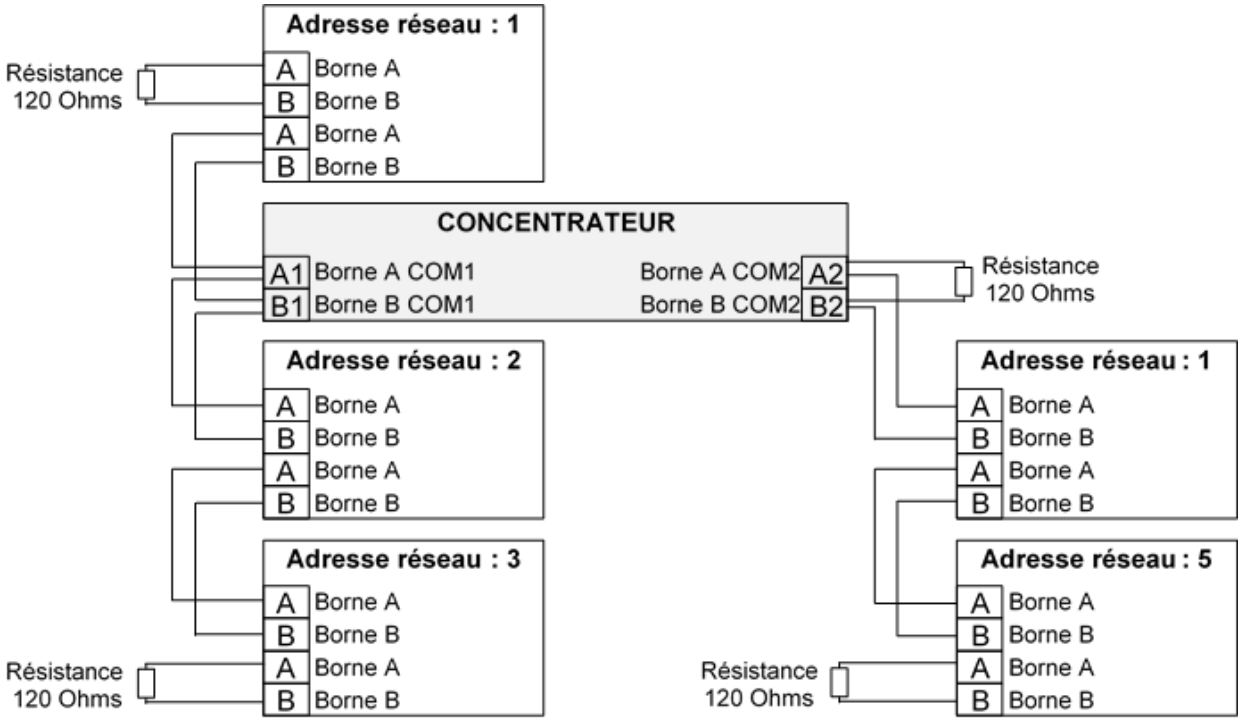


+	Entrée alimentation +12V DC	RL5	Contact relais 5
-	Entrée alimentation 0V	RL5	
RL1	Contact relais 1	RL6	Contact relais 6
RL1		RL6	
RL2	Contact relais 2	RL7	Contact relais 7
RL2		RL7	
RL3	Contact relais 3	RL8	Contact relais 8
RL3		RL8	
RL4	Contact relais 4		
RL4			

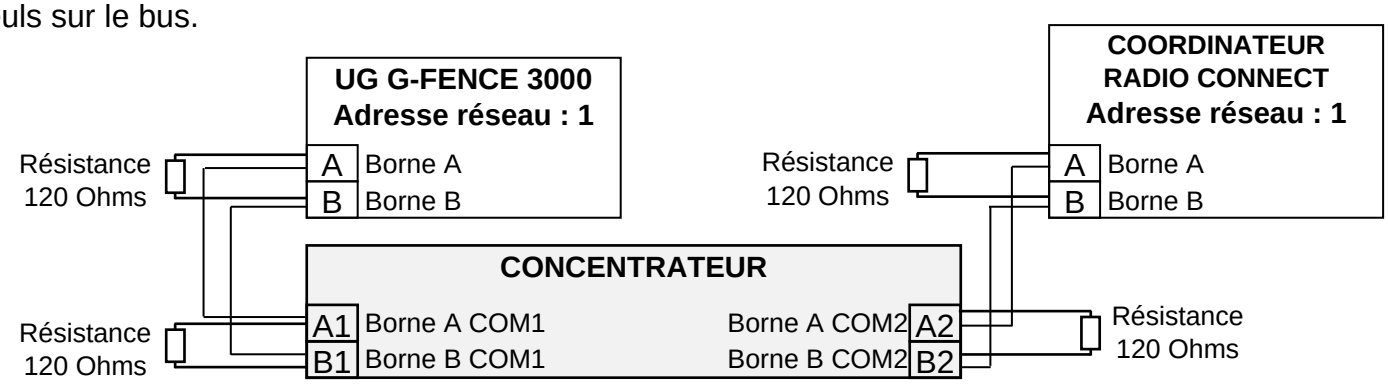
3.3 Raccordement aux équipements

La mise en réseau des produits (exemple : MAXIRIS 3000 / 3100, PIRAMID CONNECT, MODULE CONNECT…) à l'aide du concentrateur MAXIBUS UNIVERSEL forme un bus série.
Il est nécessaire de raccorder une résistance de 120 Ohms ¼ Watt aux deux extrémités d'une branche.
Il faut affecter une adresse réseau différente à chaque produit câblé sur le bus (se référer aux notices de paramétrage de chacun des produits câblés sur le bus).
Les adresses réseaux doivent être uniques sur un même port COM.

Exemple de produits raccordés sur deux ports COM :



Nota : L'Unité de Gestion G-FENCE 3000 et le COORDINATEUR RADIO CONNECT doivent être seuls sur le bus.



4 CONCENTRATEUR

4.1 Configuration du PC de l'utilisateur

Par défaut, les paramètres de connexion du concentrateur MAXIBUS UNIVERSEL sont les suivants :

Adresse IP	192.168.105.202
Masque sous réseau	255.255.255.0

La procédure qui suit permet de configurer le PC de l'utilisateur pour pouvoir se connecter aux produits :

Sous Windows* 7 et 8 :

- Aller dans **Panneau de configuration**, double-cliquer sur **Centre Réseau et partage**, puis à gauche sélectionner **Modifier les paramètres de la carte**, puis double-cliquer **Connexion au réseau local**.
- Dans l'onglet **Gestion de réseau**, mettre en surbrillance la ligne **Protocole Internet version 4 (TCP/IPv4)**, puis cliquer sur **Propriétés.**
- Sélectionner l'option **Utiliser l'adresse IP suivante** et entrer les paramètres réseau ci-dessous.

Sous Windows* 10 :

- Aller dans **Paramètre**, double-cliquer sur **Réseau et Internet**, puis à gauche sélectionner **Ethernet**, puis à droite **Modifier les options d'adaptateur**.
- Double-cliquer sur **Ethernet**.
- Dans **Propriétés**, mettre en surbrillance la ligne **Protocole Internet version 4 (TCP/IPv4)**, puis cliquer sur **Propriétés.**
- Sélectionner l'option **Utiliser l'adresse IP suivante** et entrer les paramètres réseau ci-dessous.

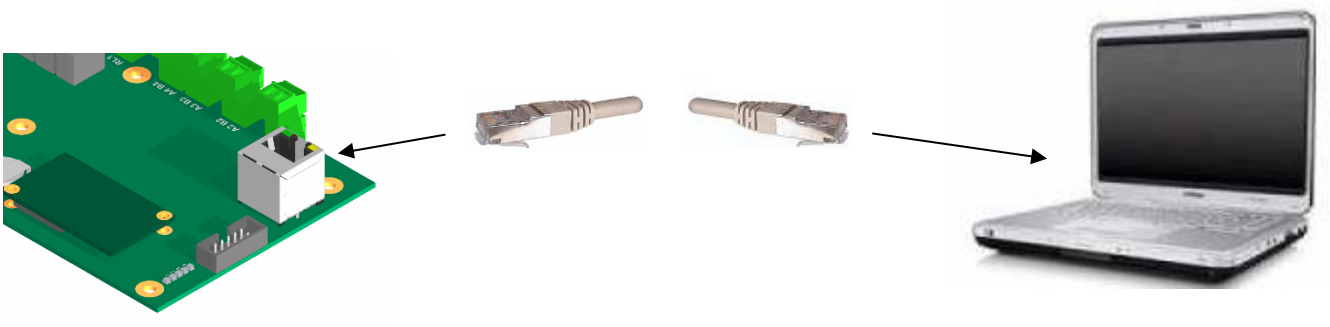
Paramètre réseau :

Paramètres	**Valeur**	**Remarques**
Adresse IP	192.168.105.XX	Le dernier nombre doit être compris entre 1 et 254 (différent de 202)
Masque sous réseau	255.255.255.0	Valeur impérative

* Windows est une marque Microsoft Corporation

4.2 Connexion au concentrateur MAXIBUS UNIVERSEL

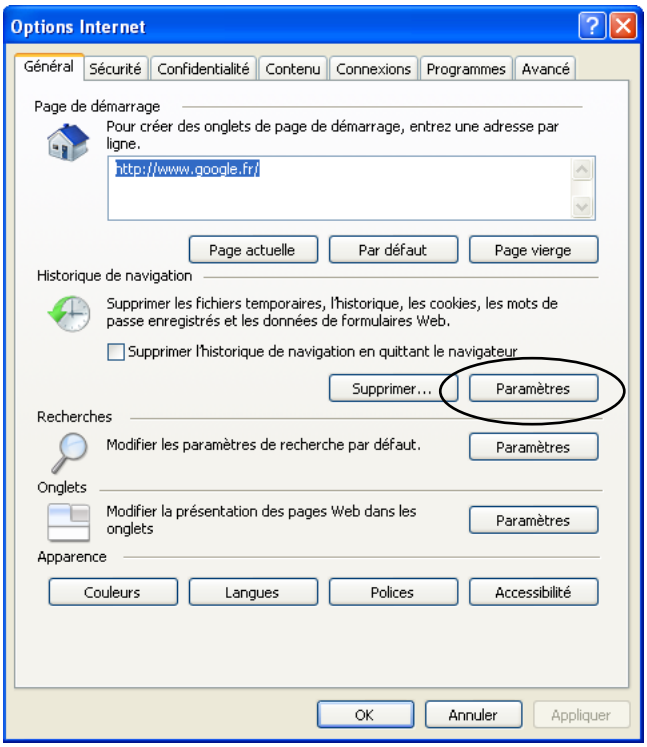
1. Connecter le PC au concentrateur MAXIBUS UNIVERSEL à l'aide d'un câble RJ45.



2. Ouvrir le navigateur internet

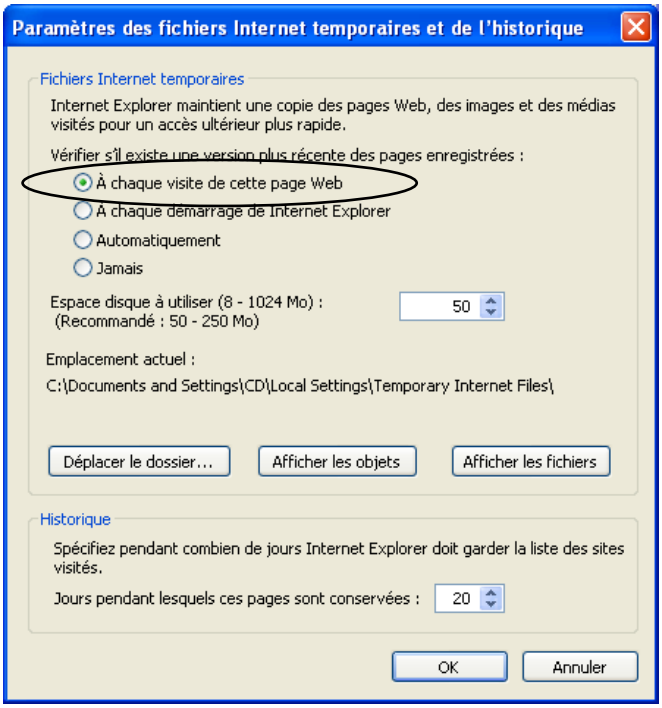
⚠ Privilégier les navigateurs Chrome, Firefox et Edge
Les pages web ne sont pas compatibles avec Internet Explorer*

3. Configuration du navigateur internet :
   - Choisir « **Outil** » dans « **Option internet** »
   - Se positionner dans l'onglet « **Général** »
   - Dans le paragraphe « Historique de navigation », cliquer sur « **Paramètres** »

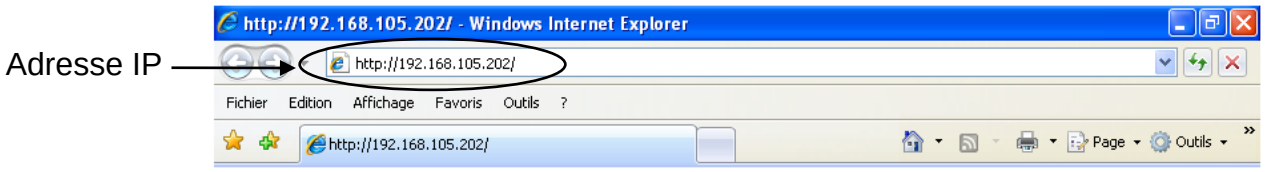


* Internet explorer est une marque Microsoft Corporation

– Vérifier que le paramètre « A chaque visite de cette page web » est validé.



4. Entrer l'adresse IP du concentrateur MAXIBUS UNIVERSEL dans l'URL du navigateur. (Par défaut : **192.168.105.202**)

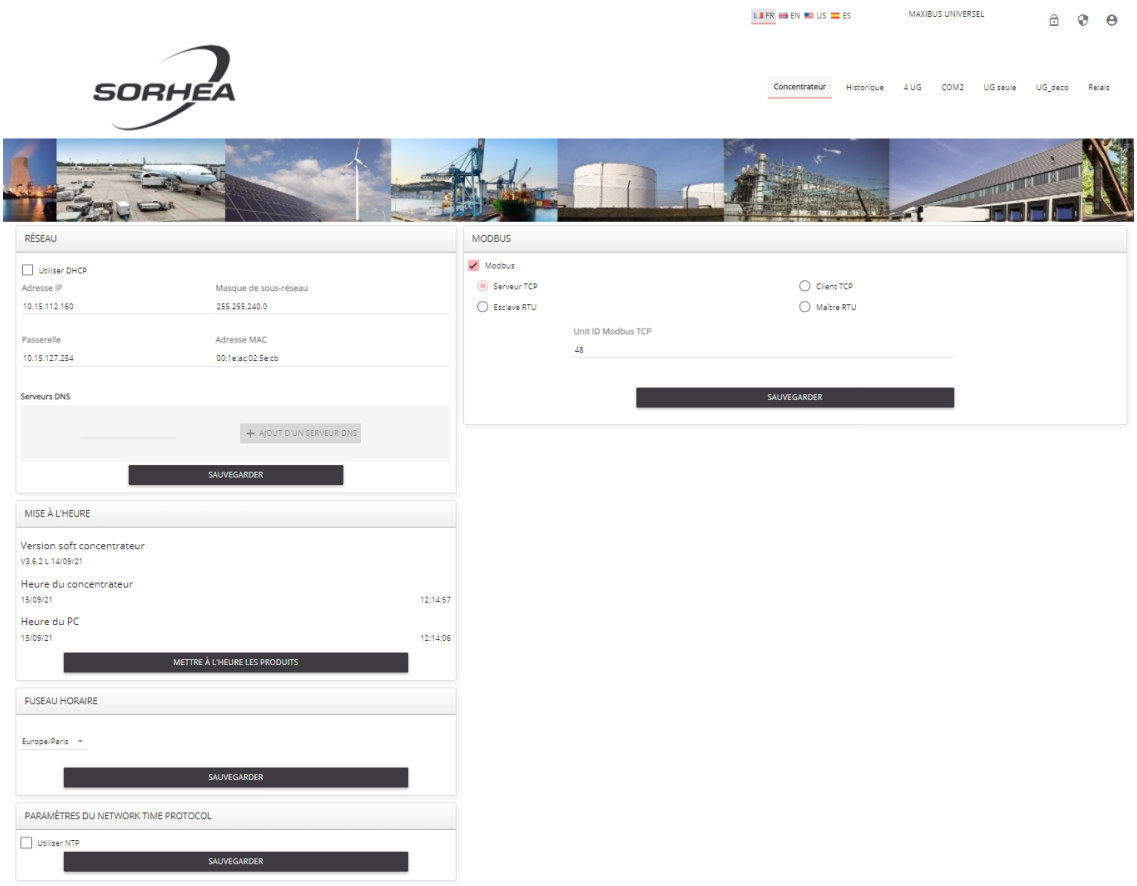


5. Entrer l'identifiant et le mot de passe (gestion de 2 niveaux de connexion) :

Type d'accès : Accès en lecture seule	
Identifiant	user
Mot de passe	0000
Type d'accès : Accès en lecture et en écriture	
Identifiant	admin
Mot de passe	␣␣␣␣ (4 espaces)

Une fois le mot de passe validé, on accède à l'ensemble des onglets du serveur web permettant de naviguer dans les différentes fonctionnalités du concentrateur MAXIBUS UNIVERSEL.

Page d'accueil :

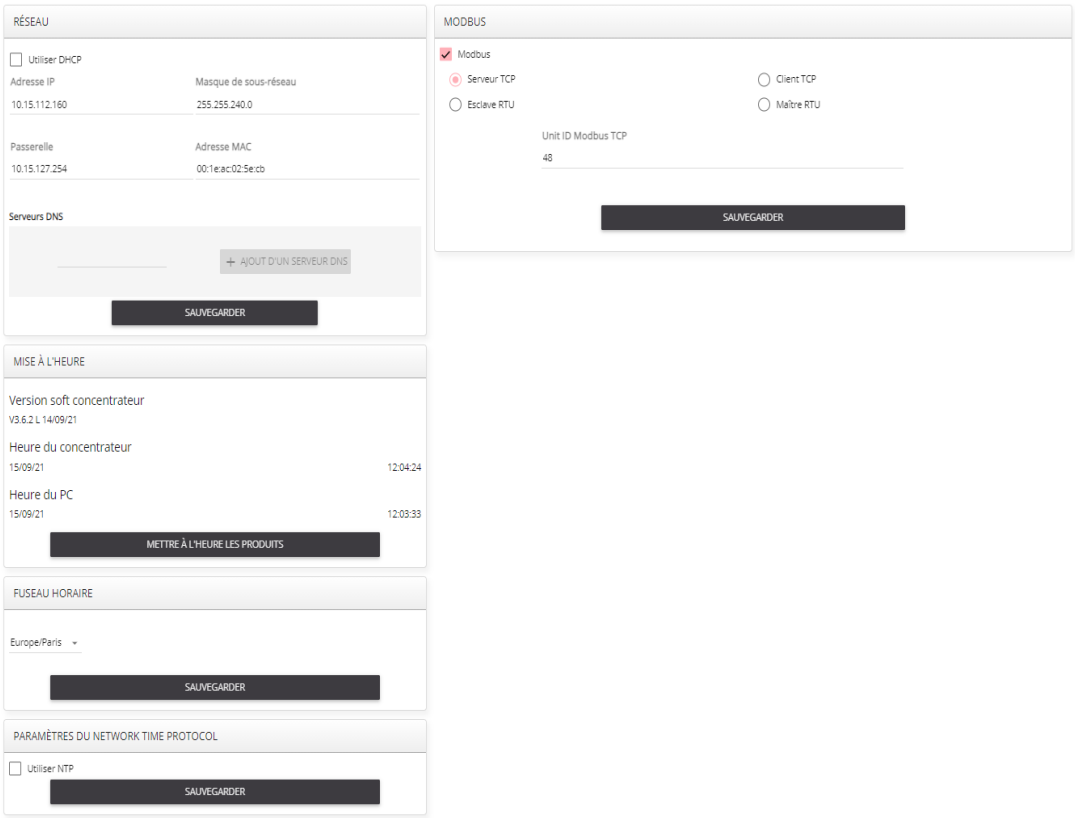


4.3 Modification des paramètres du concentrateur MAXIBUS UNIVERSEL

Nota : Pour modification des paramètres du concentrateur MAXIBUS UNIVERSEL, se connecter en « **admin** ».

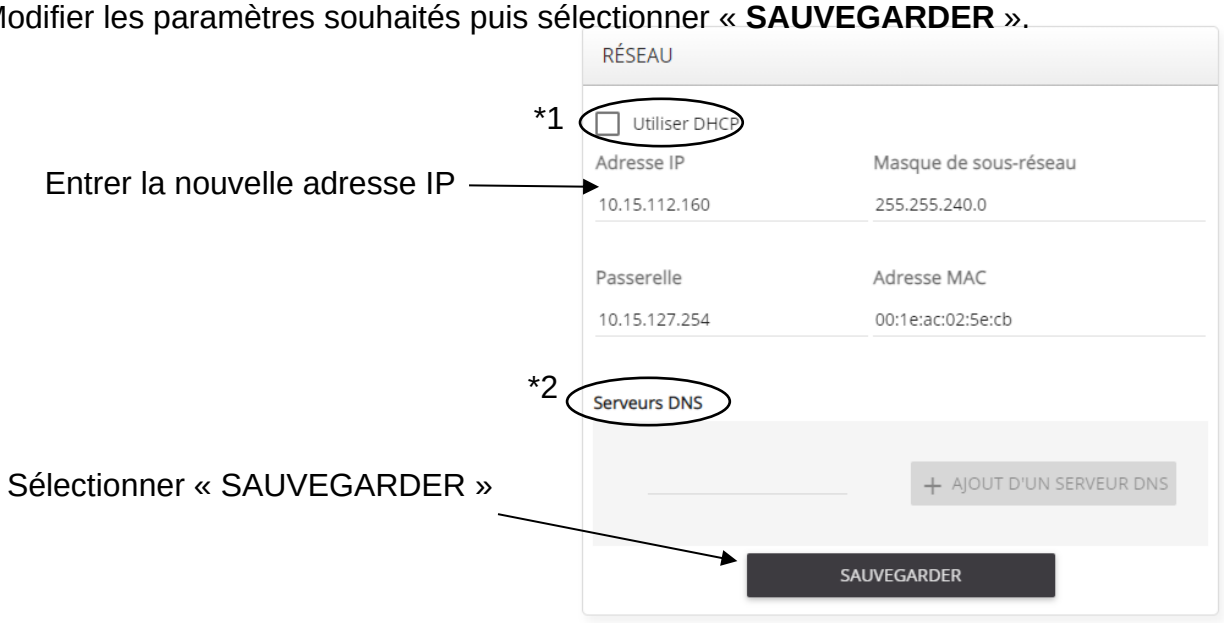
Configuration du réseau (cf. §4.3.1)

Mise à l'heure (cf. §4.3.2)



4.3.1 Configuration du réseau

1. Modifier les paramètres souhaités puis sélectionner « **SAUVEGARDER** ».



2. Attendre le rafraichissement de la page à la nouvelle adresse IP.

1 Utilisation du DHCP :

En cas d'utilisation du DHCP, le serveur affecte automatiquement une nouvelle adresse IP au MAXIBUS. La redirection sur la nouvelle adresse IP ne peut donc pas être automatique, il faut se rapprocher d'un administrateur réseau pour retrouver la nouvelle adresse du MAXIBUS.

Une fois la nouvelle IP trouvée, une pastille verte indiquera à l'utilisateur que le DHCP est fonctionnel. Si la pastille est rouge, cela signifie que le MAXIBUS n'a pas pu récupérer une nouvelle adresse auprès d'un serveur.

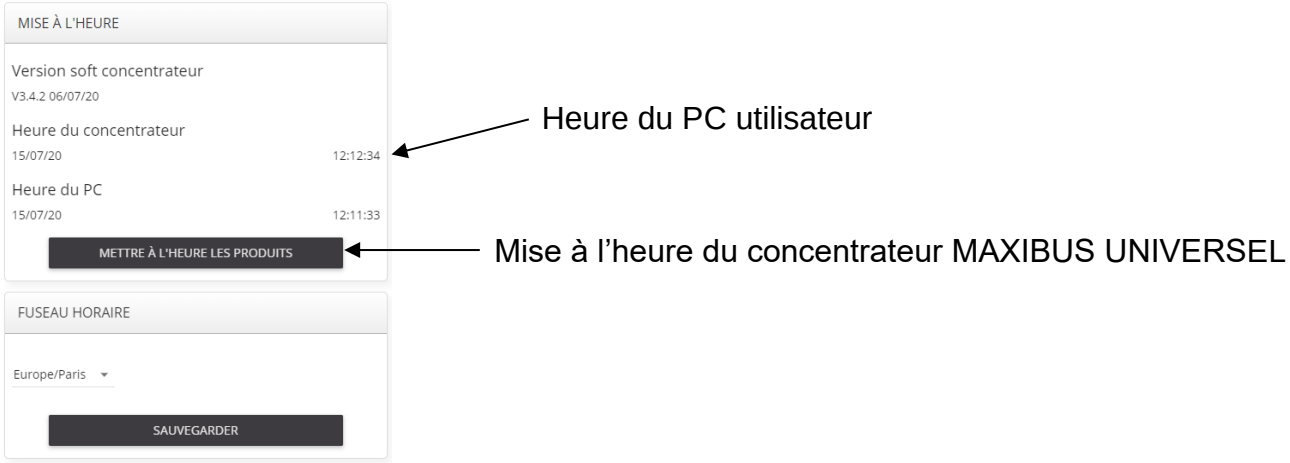
2 Utilisation d'un serveur DNS :

L'utilisateur a la possibilité de configurer un (ou deux) serveurs DNS sur le MAXIBUS.
Les fonctionnalités du DNS sont pour le moment limitées à la configuration d'un serveur NTP utilisant un nom de domaine (voir partie 4.3.2).

4.3.2 Mise à l'heure du concentrateur MAXIBUS UNIVERSEL

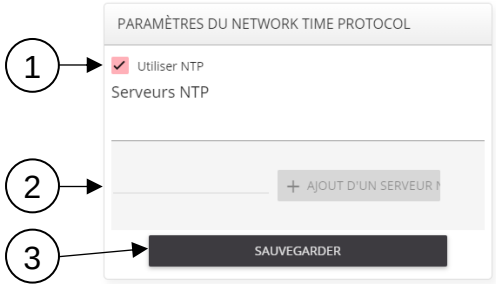
Mise à l'heure manuelle :

Sélectionner « **METTRE A L'HEURE LES PRODUITS** » pour mettre à l'heure le concentrateur avec l'heure du PC utilisateur.



Mise à l'heure automatique par NTP :

Il est possible de synchroniser l'heure du MAXIBUS sur des serveurs de temps.
Cette synchronisation utilise le protocole NTP.



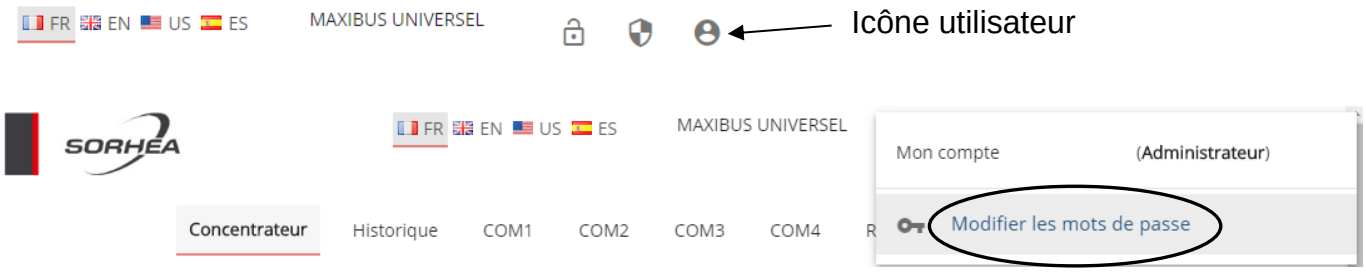
1. Cliquer sur la case pour activer le NTP.
2. Ajouter l'adresse du serveur NTP et cliquer sur « + AJOUT D'UN SERVEUR NTP ».
3. Cliquer sur « Sauvegarder ».

Remarque :

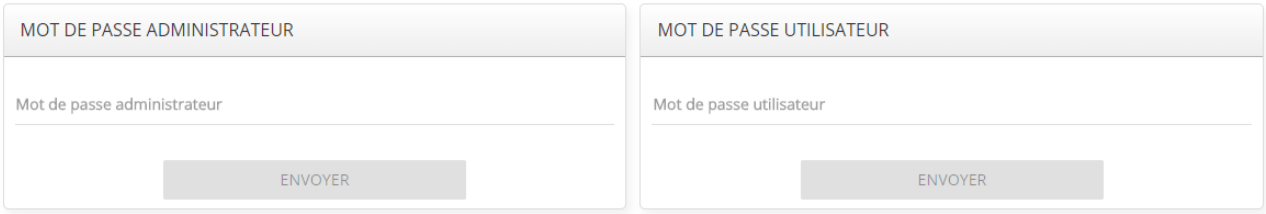
Le NTP peut être activé via un serveur en utilisant l'adresse IP ou bien le nom de domaine du serveur.
L'ajout d'un serveur NTP avec nom de domaine requiert, au préalable, l'activation d'un serveur DNS (voir la partie 4.3.1).

4.3.3 Modification des mots de passe

1. Sélectionner l'icône utilisateur en haut de page puis sélectionner « **MODIFIER LES MOTS DE PASSE** »



2. Entrer le nouveau mot de passe qui doit être modifié dans la case « Mot de passe administrateur » pour le login « **ADMIN** » ou dans la case « Mot de passe utilisateur » pour le login « **USER** » puis appuyer sur le bouton « **ENVOYER** » correspondant.



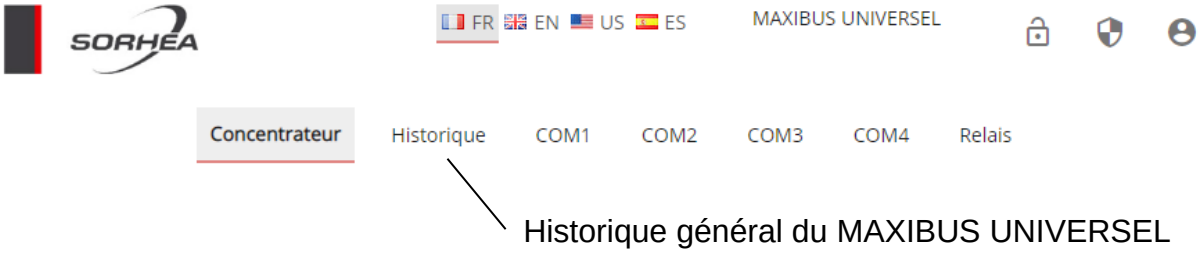
   Nota : le mot de passe peut contenir 30 caractères maximum.

3. Attendre le rafraichissement de la page puis sélectionner « **Concentrateur** » pour revenir à la page d'accueil.

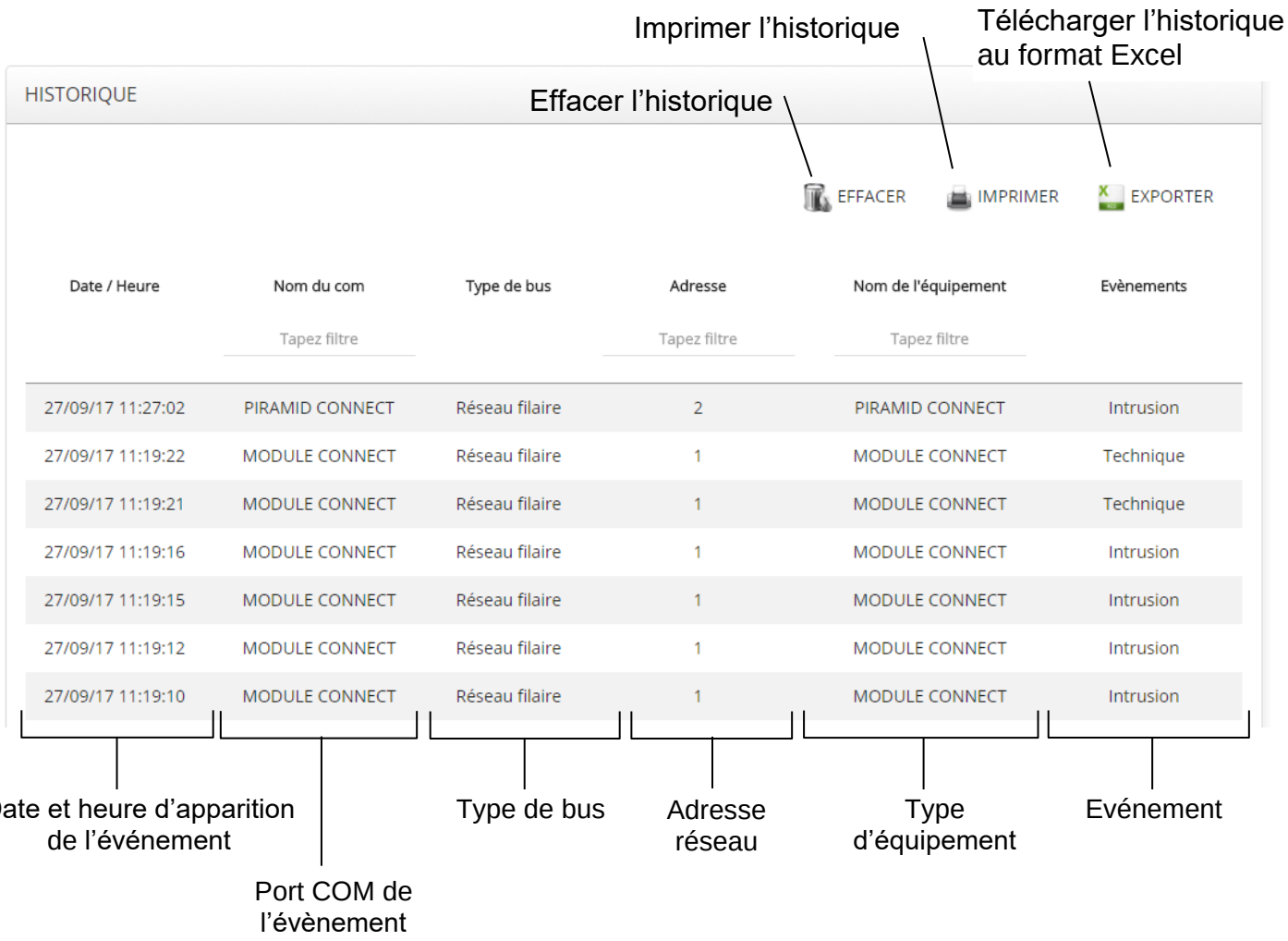
4.4 Consultation de l'historique générale du CONCENTRATEUR MAXIBUS UNIVERSEL

Cet historique permet l'affichage d'une synthèse des évènements de l'ensemble du site.
On retrouve uniquement les informations d'alarme technique et intrusion des produits connectés ainsi que les modifications de configuration du concentrateur.

Cliquer sur l'onglet « **Historique** ».



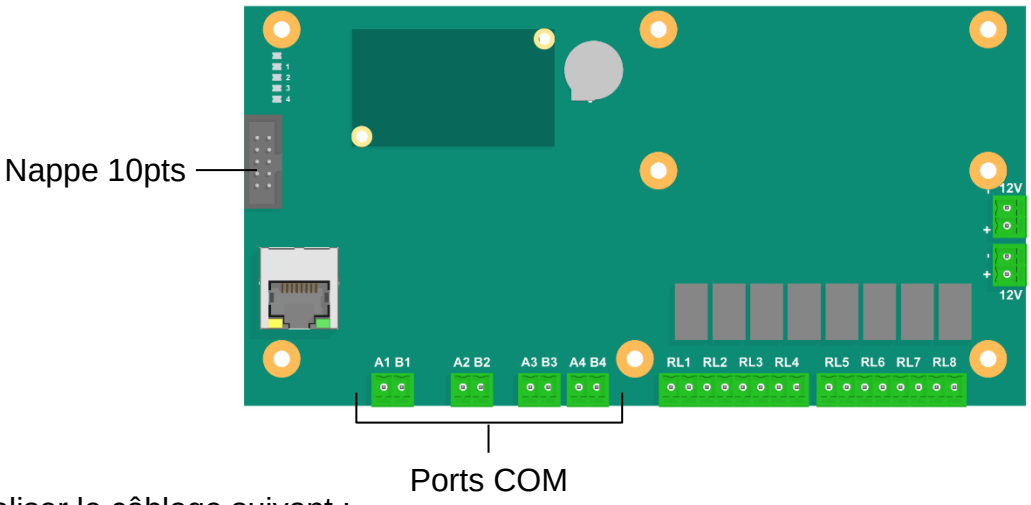
Détail de l'historique :



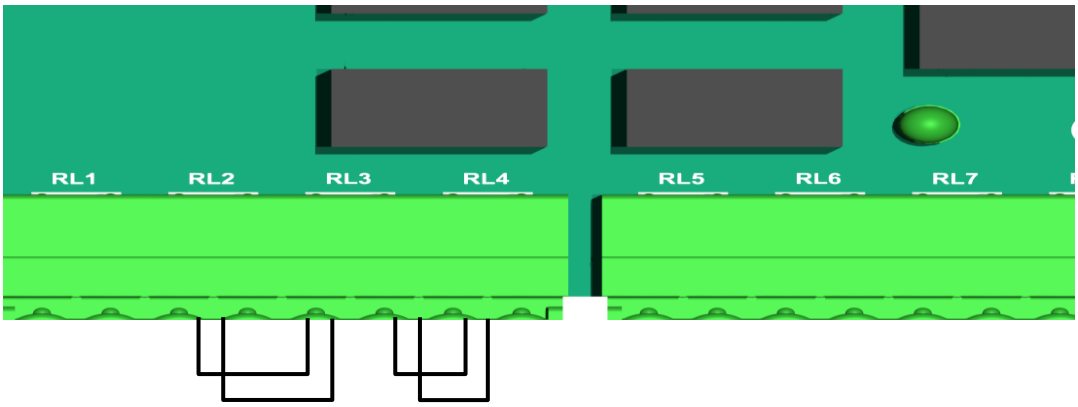
4.5 Procédure de reset de l'adresse IP du concentrateur MAXIBUS UNIVERSEL

Si l'adresse IP du concentrateur MAXIBUS UNIVERSEL modifiée par l'utilisateur est perdue, la procédure suivante permet un retour au paramétrage IP d'usine.

1. Mettre le concentrateur MAXIBUS UNIVERSEL hors tension.
2. Débrancher le ou les ports COM connectés.
   Débrancher la nappe 10pts de liaison entre le concentrateur MAXIBUS UNIVERSEL et les cartes extension 8 relais.
   Débrancher le connecteur RJ45 et les relais.



3. Réaliser le câblage suivant :



4. Mettre sous tension le concentrateur MAXIBUS UNIVERSEL et attendre la séquence suivante :

   Le voyant vert L0 est allumé fixe.
   Les voyants L1 à L4 sont en chenillard.

5. Défaire le câblage réalisé à l'étape 3 et attendre la fin du chenillard.

6. Rebrancher le connecteur RJ45 puis se connecter sur http://192.168.105.202/

7. Rebrancher le ou les ports COM connectés.
   Rebrancher la nappe 10pts de liaison entre le concentrateur MAXIBUS UNIVERSEL et les cartes relais extension.
   Rebrancher les relais.

8. Faire une mise à jour de la date et de l'heure. (cf. §4.3.2)

4.6 Procédure de remplacement de la pile mémoire

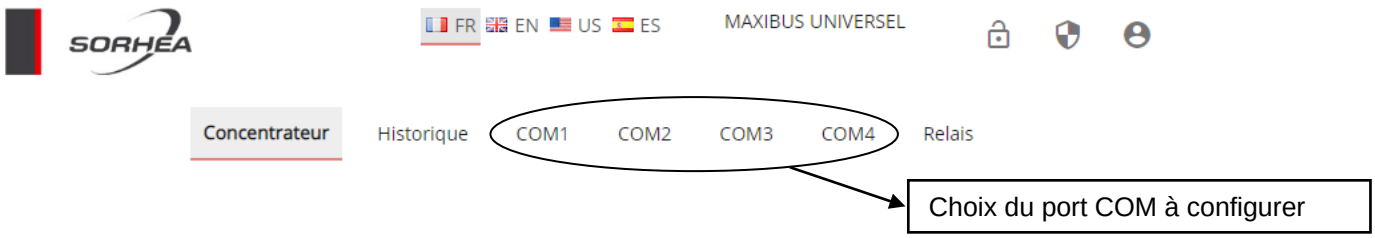
La pile mémoire a une durée de vie en moyenne de **10 ans**.

Faire une sauvegarde de la configuration du site et des paramètres des relais en fin de paramétrage du site. (Voir §5.4.1)
Lorsque la pile mémoire est déchargée, remplacer la carte concentrateur MAXIBUS UNIVERSEL et charger la configuration du site et des relais. (Voir §5.4.2)

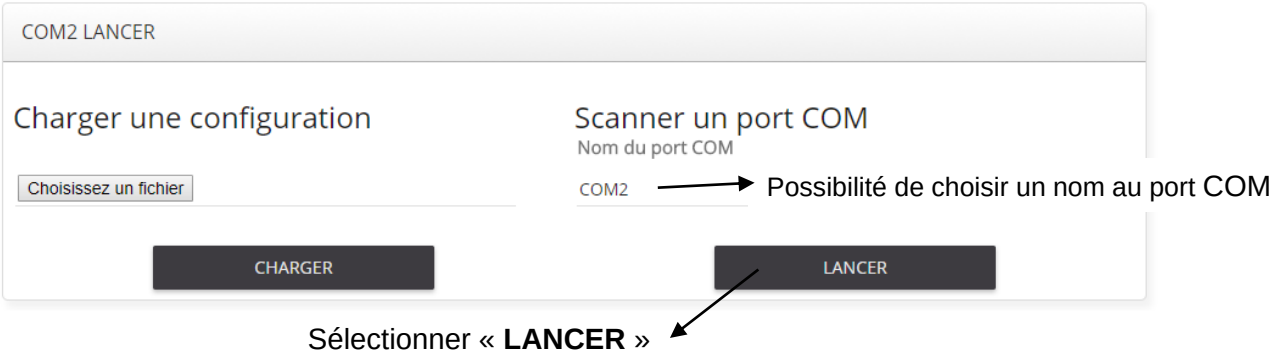
5 GESTION DES PORTS COM

5.1 Configuration du port COM

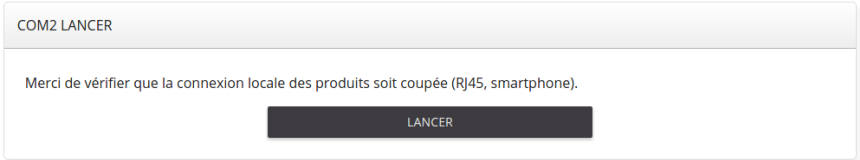
1. Cliquer sur le port COM à configurer.



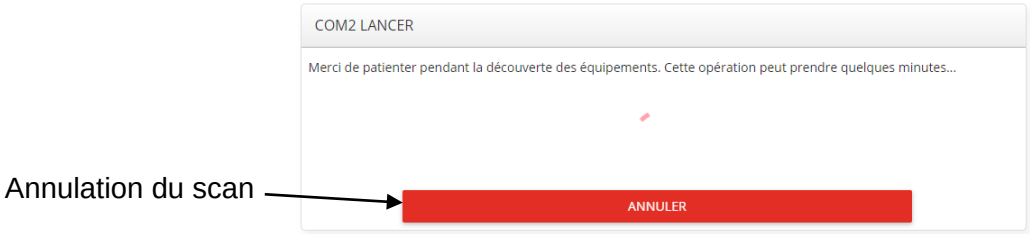
2. Sélectionner « LANCER » pour démarrer la configuration du port COM.
   Nota : Possibilité de choisir un nom au port COM (par défaut, le nom du port COM est celui du type de produit)



3. Vérifier que la connexion locale des produits soit coupée : débrancher la liaison RJ45, fermer l'application smartphone. Cliquer sur Lancer.

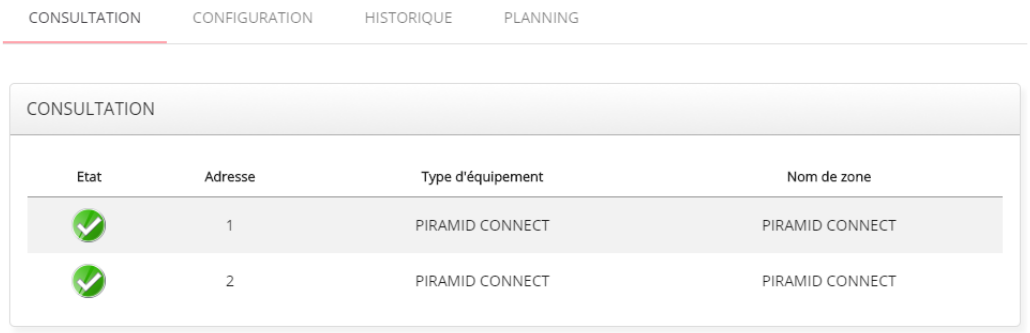


4. Attendre le chargement de la page de lancement de la configuration.
   Patienter pendant le temps du scan.



5. La liste du matériel reconnu apparait.
   Se reporter à la notice des produits pour l'utilisation.

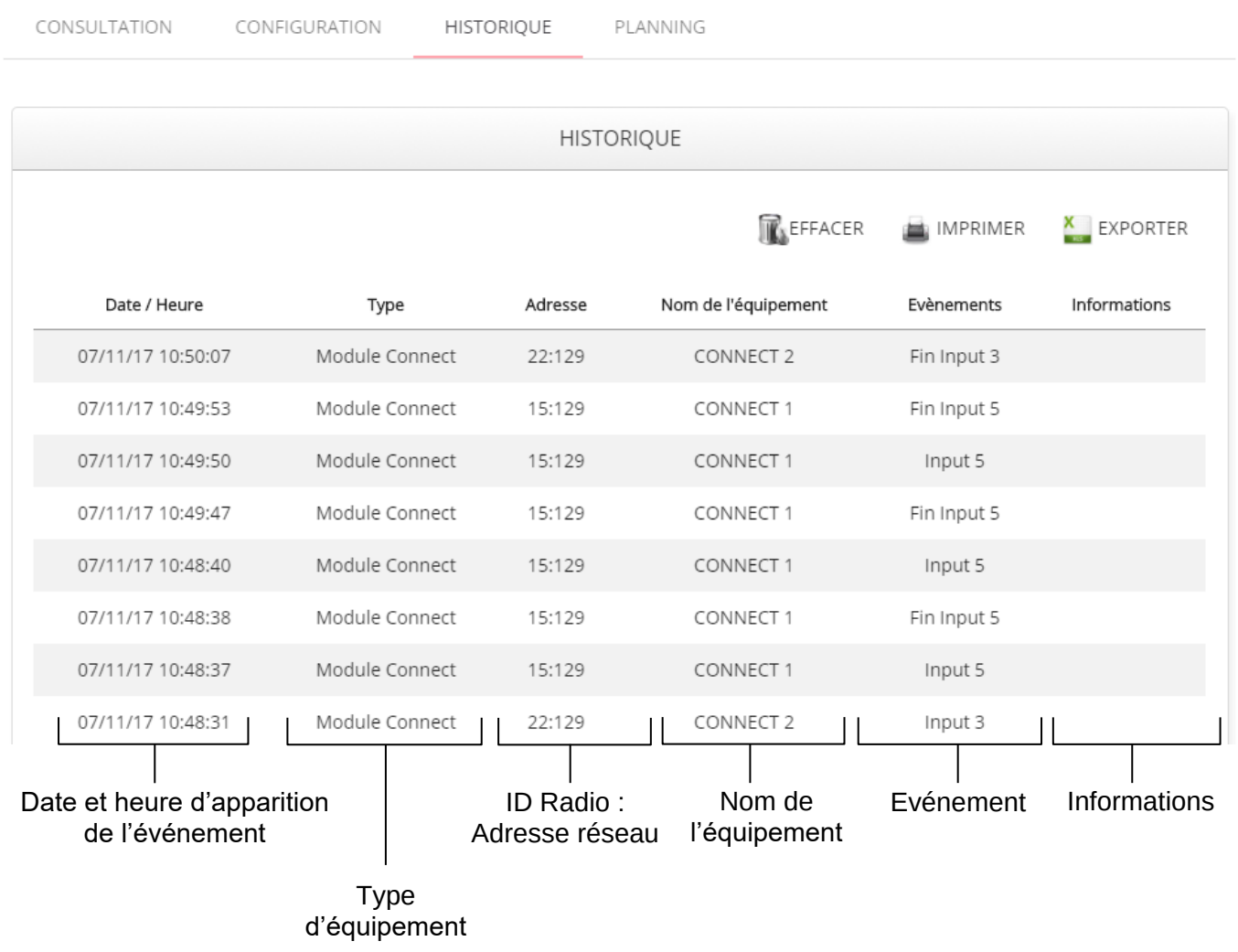
Exemple d'écran qui apparait à la fin de la recherche :



5.2 Historique du port COM

Cet historique permet l'affichage d'une synthèse des évènements de l'ensemble du port COM.

Exemple d'historique :



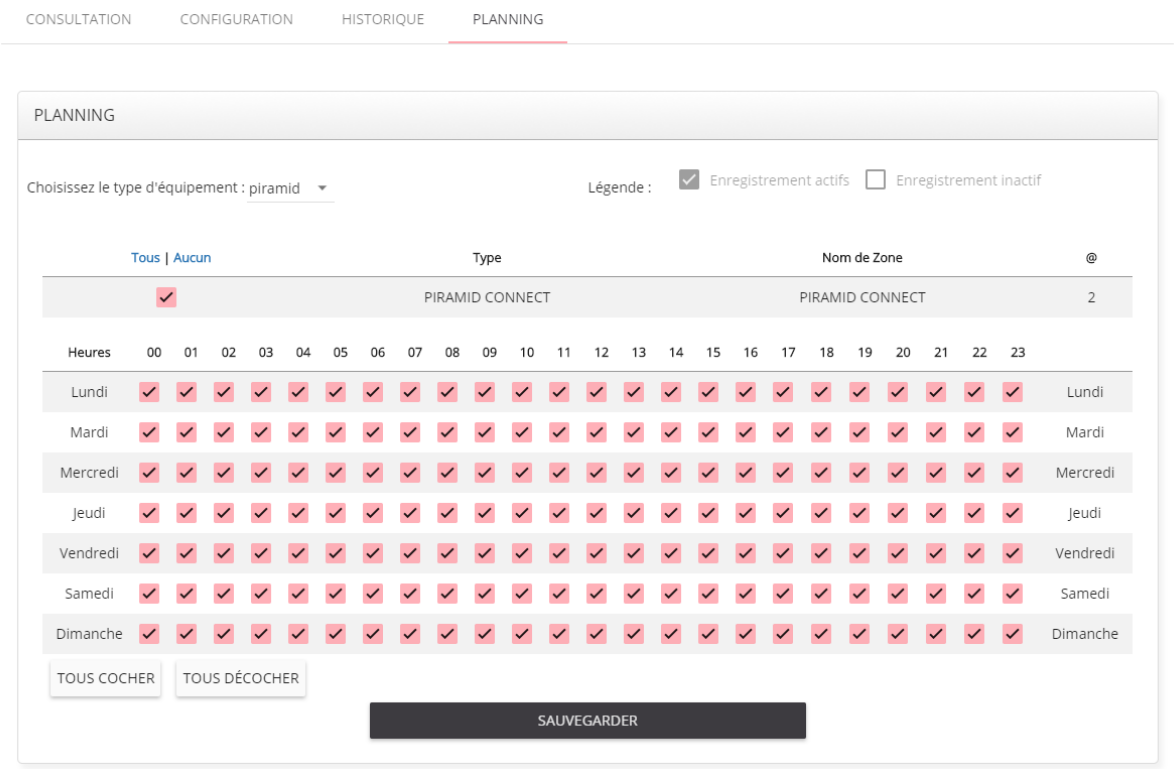
5.3 Gestion du planning spécifique de l'historique

Objectif : ne plus enregistrer les alarmes sélectionnées dans l'historique, toutefois les sorties d'alarme restent actives.

Nota : par défaut, toutes les alarmes des éléments connectés sur le concentrateur MAXIBUS UNIVERSEL sont enregistrées dans l'historique.

- Aller dans le port COM dont le planning doit être configuré.
- Sélectionner « **PLANNING** ».
- Par défaut, tous les éléments sont cochés.

1. Sélectionner l'élément dont le planning doit être spécifique.
2. Choisir les périodes d'enregistrement et de non enregistrement de l'élément.
3. Sélectionner « **ENVOYER** »



Note : pour les éléments non sélectionnés, l'enregistrement est permanent.

5.4 Sauvegarde et chargement de la configuration d'un port COM

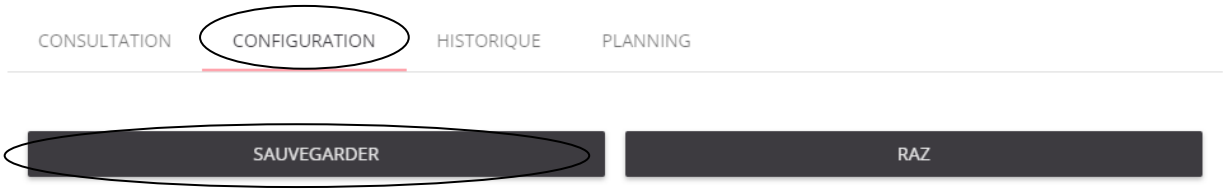
Chaque port COM du concentrateur MAXIBUS UNIVERSEL peut être sauvegardé indépendamment. Le concentrateur MAXIBUS UNIVERSEL sauvegarde :

1. La configuration du port COM
2. L'affectation des relais du port COM
3. La configuration du site lié au port COM

Il est possible de sauvegarder cette configuration à partir du concentrateur MAXIBUS UNIVERSEL, et de la restituer.

5.4.1 Sauvegarde de la configuration du concentrateur MAXIBUS UNIVERSEL

- Aller dans le port COM à sauvegarder.
- Sélectionner « **CONFIGURATION** », puis « **SAUVEGARDER** ».

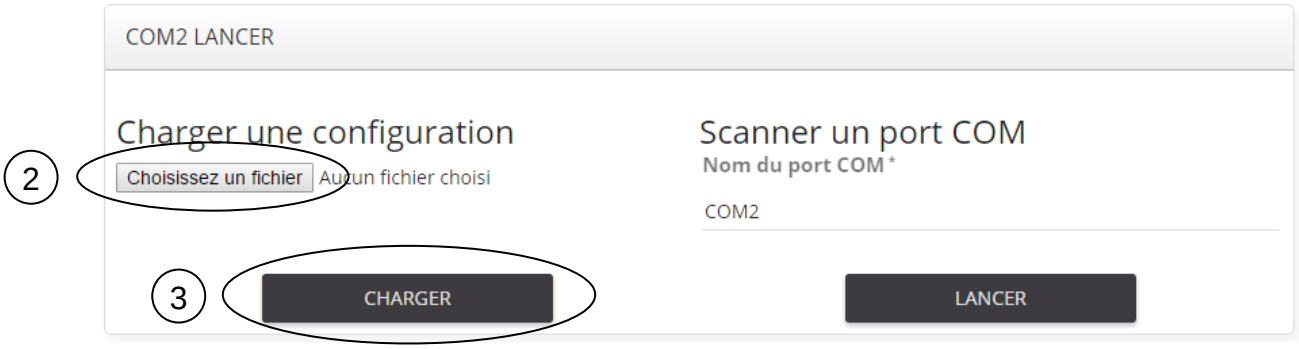


- Le fichier « NETWORKx.conf » (x numéro du port COM) se télécharge.

5.4.2 Chargement de la configuration dans le concentrateur MAXIBUS UNIVERSEL

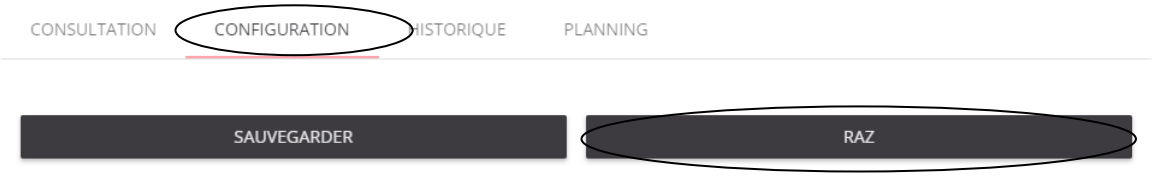
Nota : pour faire un chargement de configuration d'un port COM, il faut que celui-ci ne soit pas configuré. (Voir §5.5 Effacement de la configuration d'un port COM)

1. Cliquer sur le port COM à configurer.
2. Choisir le fichier à charger
3. Cliquer sur le bouton CHARGER



5.5 Effacement de la configuration d'un port COM

- Aller dans le port COM dont la configuration est à effacer.
- Sélectionner « **CONFIGURATION** », puis « **RAZ** ».



- Confirmer l'effacement de la configuration du port COM.

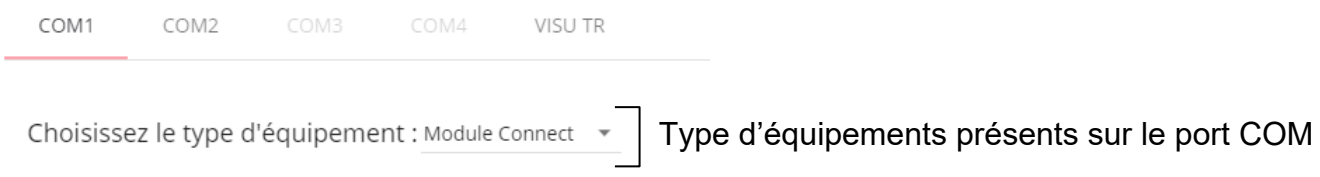
6 GESTION DES SORTIES DES ALARMES

6.1 Affectation des sorties relais

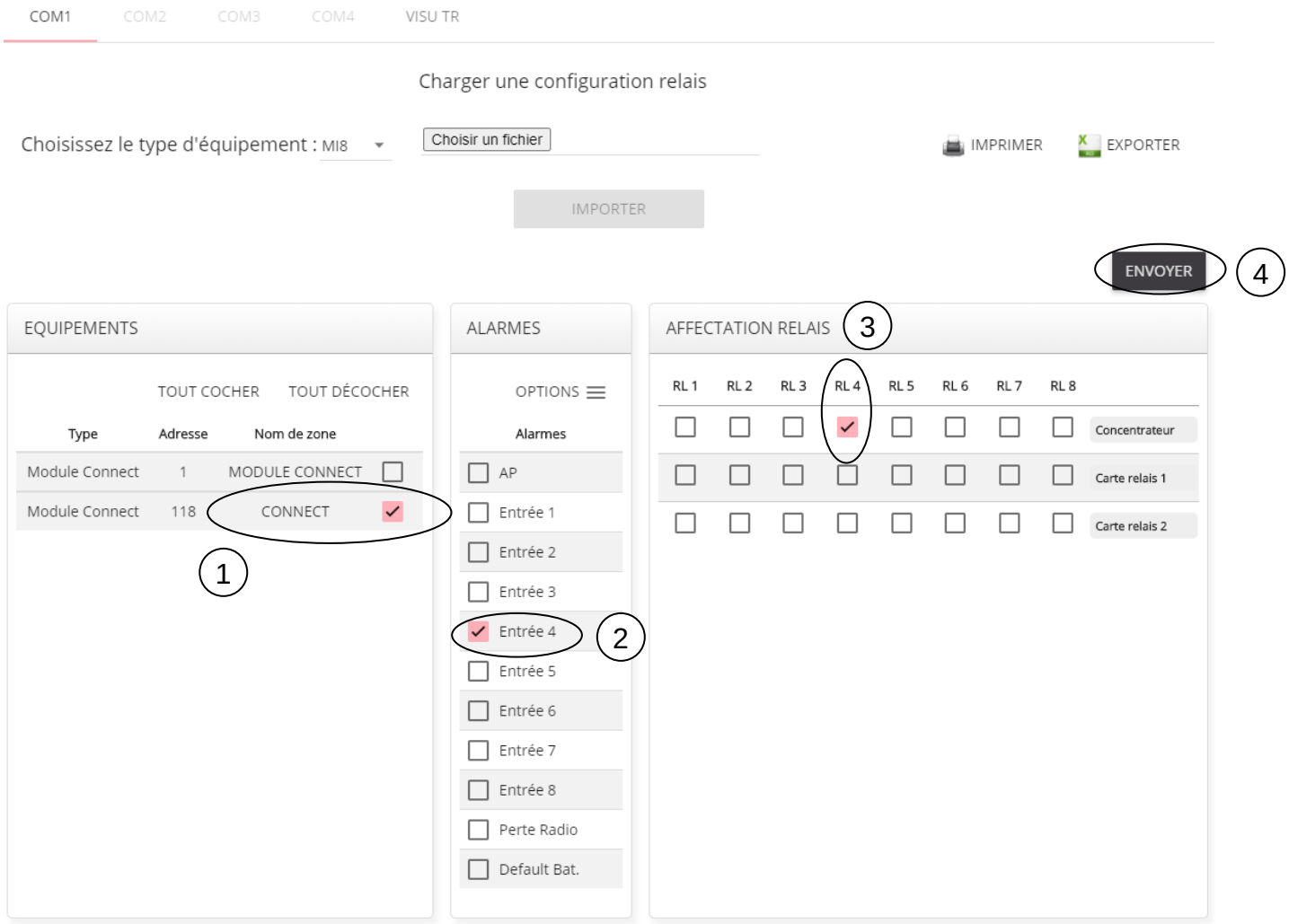
<u>Procédure d'affectation des relais</u> :

- Sélectionner « **Relais** », puis en haut de page sélectionner le port COM sur lequel s'effectue l'affectation des relais.

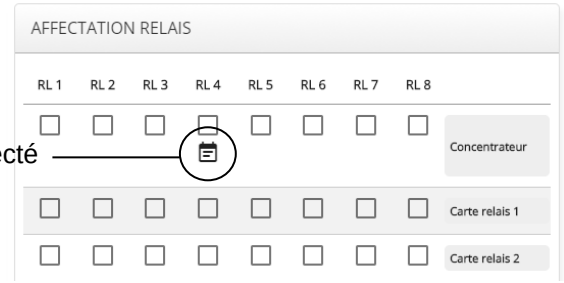
- Sélectionner le type d'équipement.



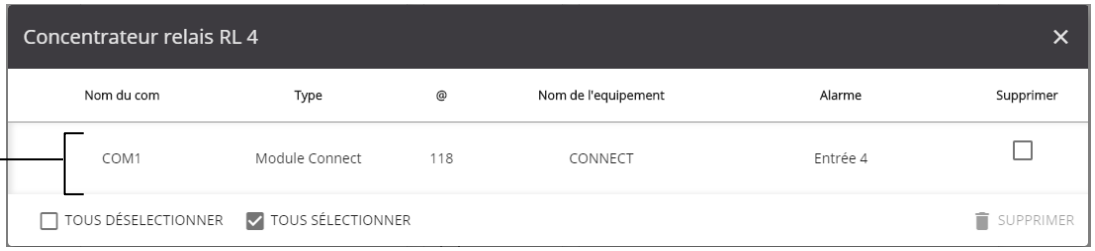
- Affecter les relais :
    1. Sélectionner l'équipement dont les alarmes sont à affecter.
    2. Sélectionner l'alarme à affecter aux relais.
    3. Sélectionner le (ou les) relais sur lequel sera affectée l'alarme.
    4. Sélectionner « **ENVOYER** ».



- Un symbole apparaît en dessous du relais affecté.
  Cliquer sur le symbole pour connaître la liste des alarmes affectées à ce relais.

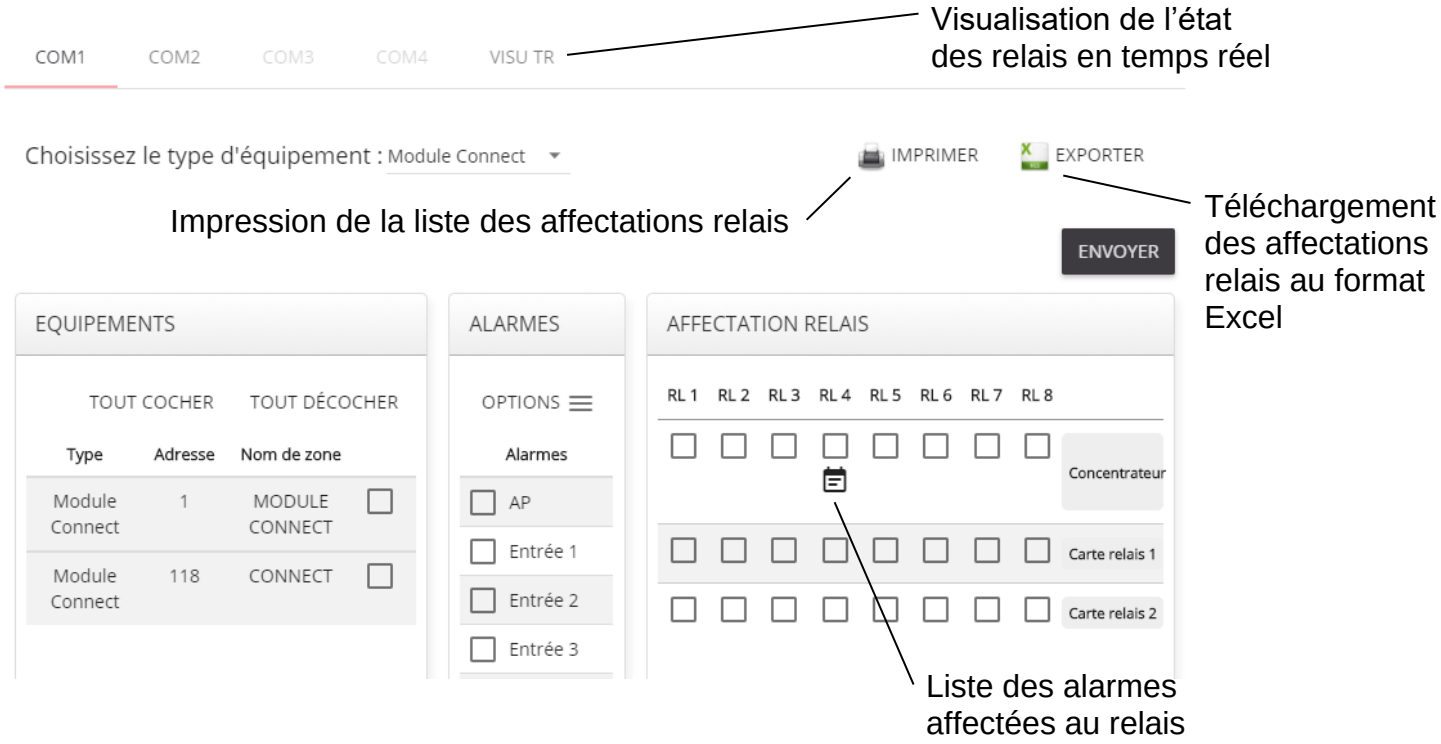


Relais affecté

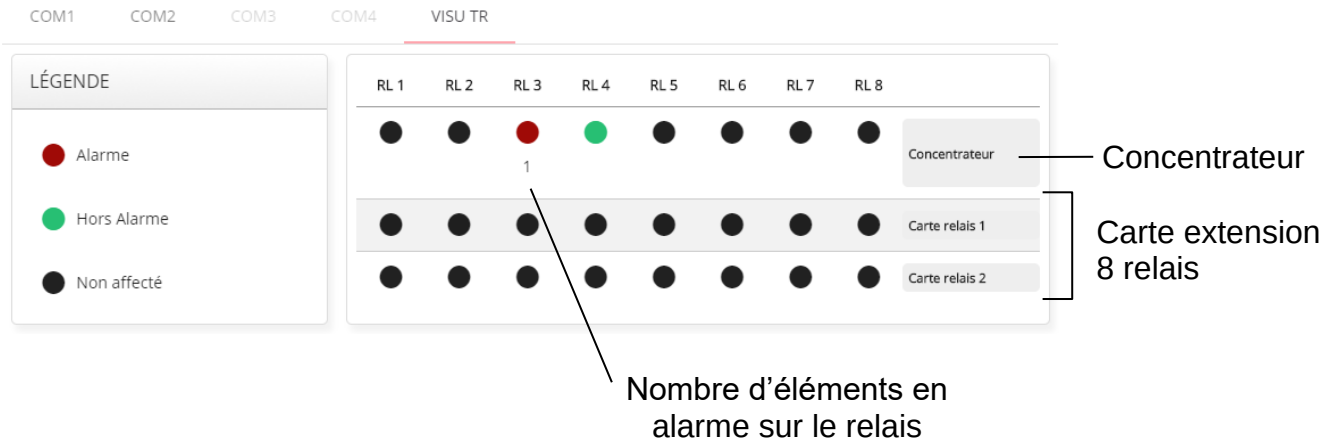


Liste des alarmes affectées au relais

6.2 Visualisation des affectations des relais



<u>Visualisation de l'état des relais en temps réel</u> :



6.3 Sortie des alarmes par MODBUS

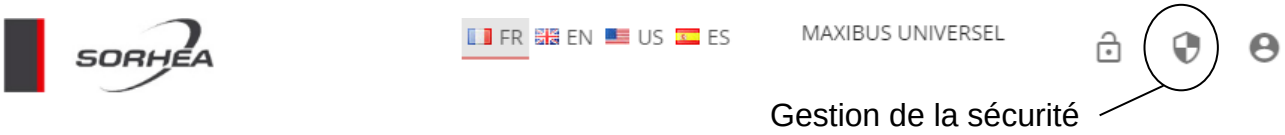
Pour utiliser la sortie des alarmes via la liaison MODBUS, voir notice du protocole de communication NT401.

6.4 Sortie des alarmes par API

Pour utiliser la sortie des alarmes via API, voir notice du protocole de communication NT424.

7 SECURISATION ETHERNET

Accéder aux pages de gestion de la sécurité, cliquer sur le bouclier :



3 Menus disponibles :

1. Configuration : configuration du certificat HTTPS et TLS
2. Certificats : gestion des certificats
3. 802.1X : configuration du contrôle d'accès aux équipements d'infrastructures réseau

7.1 Consignes de sécurité

7.1.1 Préliminaire

La mise en œuvre d'un concentrateur obéit à des règles visant à éviter les failles de sécurité aussi bien pendant la configuration qu'en exploitation.
Le respect de ces règles est fortement recommandé pour tous les sites à caractères sensibles.

7.1.2 Connexion HTTP ou HTTPS

L'interface de configuration est accessible à partir d'un navigateur Web.
En configuration Usine, et avant toute installation de certificat, la connexion sur le concentrateur est possible en HTTP. Dans ce mode, la communication n'est pas chiffrée. Il est donc fortement conseillé de se placer sur un réseau isolé pour éviter tout risque de capture des informations échangées. Dès qu'un certificat a été installé et le mode HTTPS activé, la connexion se fait uniquement en HTTPS garantissant alors la sécurité des échanges.

7.1.3 SSH

L'activation de la connexion SSH par mot de passe est fortement déconseillée car représente une faille de sécurité importante.
L'activation doit être temporaire pour éventuellement des besoins de support technique et doit être désactivée à la fin de la manipulation.

7.1.4 Procédure de première mise en sécurité d'un concentrateur

Cette section liste chronologiquement les opérations à faire en précisant l'objectif en termes de sécurité.

1. Se connecter en HTTP sur le concentrateur.
   Fixer les paramètres réseau du module : Adresse IP, Masque Réseau, ... (cf. §4.3).
   Ces informations sont normalement fournies par l'administrateur réseau du site (RSSI).

2. Générer, Signer et Installer les certificats pour HTTPS et éventuellement 802.1x
   Voir §7.2 Gestion des certificats et §7.3 802.1X qui détaillent ces opérations.
   L'objectif de cette étape est de sécuriser les échanges réseau lors de la configuration Web, des communications avec le concentrateur, et l'accès au réseau de l'entreprise dans le cas d'une infrastructure sécurisée par le protocole 802.1X.

3. Se connecter en HTTPS sur le concentrateur et changer les mots de passe par défaut par des mots de passe définitifs ou provisoires le temps du chantier.

7.2 Gestion des certificats

Cette page permet :

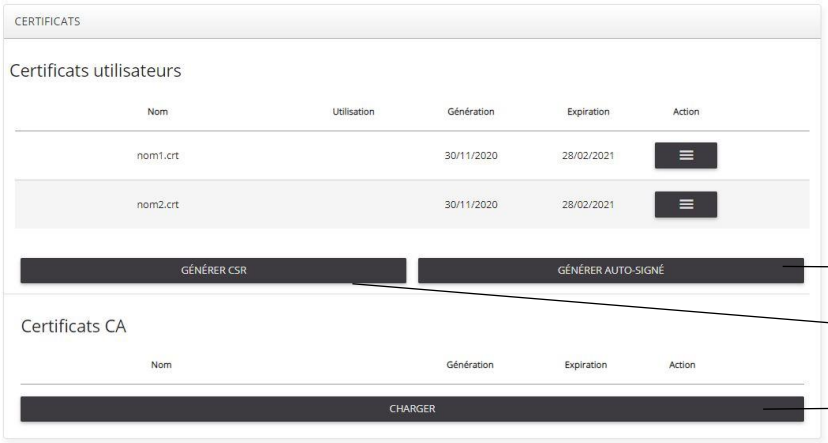
- De créer des certificats auto-signés.
- De créer et exporter des certificats CSR (En anglais « Certificate Signing Request » : certificats à faire signer par un organisme d'autorité de certification)
- D'importer un certificat signé.
- D'importer des certificats d'autorité de racine de confiance.

Ces différents certificats seront nécessaires pour utiliser une communication TLS sécurisée avec certificats auto-signés/certificats signés ou encore pour la sécurisation HTTPS de la page web.

➢ Qu'est-ce qu'un certificat ?

Un certificat numérique (ou électronique) est un fichier numérique qui va permettre de sécuriser la communication TCP entre différents appareils. Les différentes informations présentes dans le fichier vont permettre :

- De s'authentifier, pour confirmer que les appareils soient bien autorisés à communiquer entre eux pour éviter toute tentative d'intrusion.
- De tirer les clés qui permettront de chiffrer la communication entre les appareils.

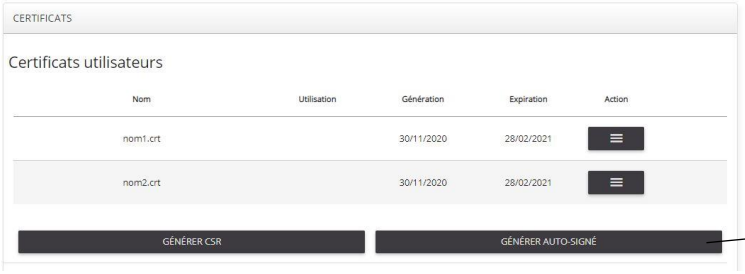


➢ Certificats auto-signés

Le certificat auto-signé est un certificat qui va être créé (avec les informations entrées par l'utilisateur) et signé par le concentrateur lui-même.

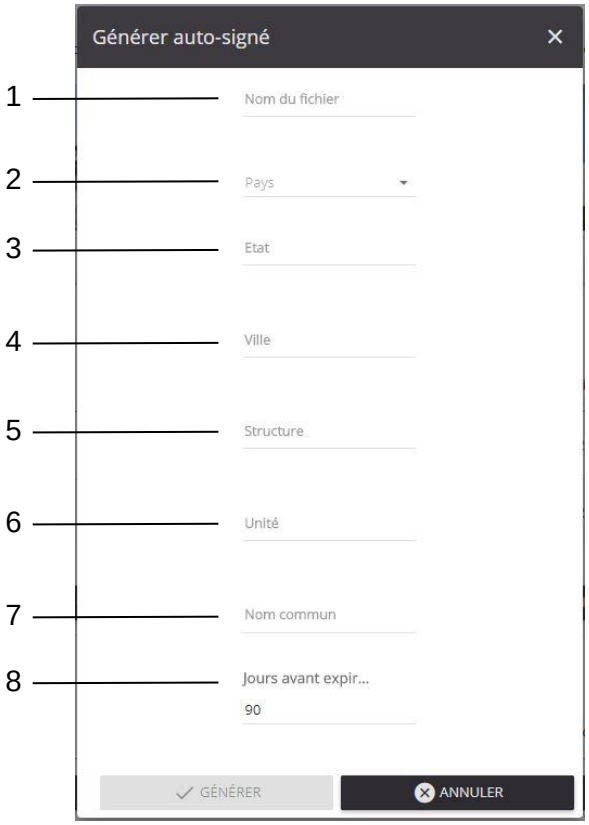
Pour générer ce type de certificat :

1. Cliquer sur le bouton « GENERER AUTO-SIGNE »



Génération des certificats auto-signés

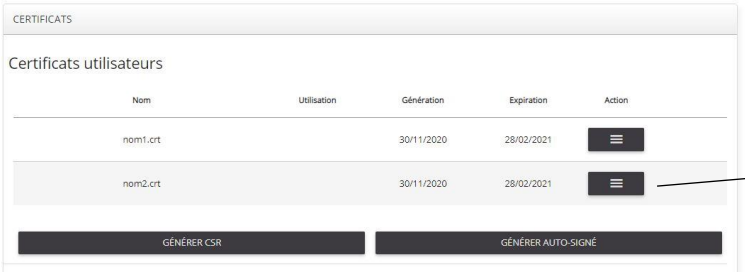
2. Remplir les informations demandées



1- Nom du fichier : nom qui sera donné au fichier généré
2- Pays : Sélectionner le pays
3- Etat : Correspond à l'état/Région/Département
4- Ville : Correspond à la ville
5- Structure : Correspond à l'entreprise
6- Unité : Correspond au service
7- Nom commun : Correspond à l'adresse IP du concentrateur ou à son nom d'hôte (host name)
8- Jours avant expiration : Correspond au nombre de jours de validité du certificat

Une fois les informations validées, une ligne se crée dans le tableau se trouvant dans la partie « Certificats utilisateurs ». Dans la première colonne on retrouve le nom du fichier que l'on a configuré et dans la dernière colonne l'indication que le certificat et en cours de création.

3. Attendre environ 1 minute pour que le certificat se génère. Lorsque les colonnes « Génération » et « Expiration » sont remplies, le certificat est prêt à être utilisé.



Le certificat est maintenant prêt à être utilisé soit dans le paramétrage pour la sécurisation de la page web HTTPS (Configuration / Security) soit pour le paramétrage de la sécurisation de la communication TCP (Configuration / Network).
Une fois le certificat utilisé par une des deux fonctions, la colonne « Utilisation » du tableau sera renseigné.

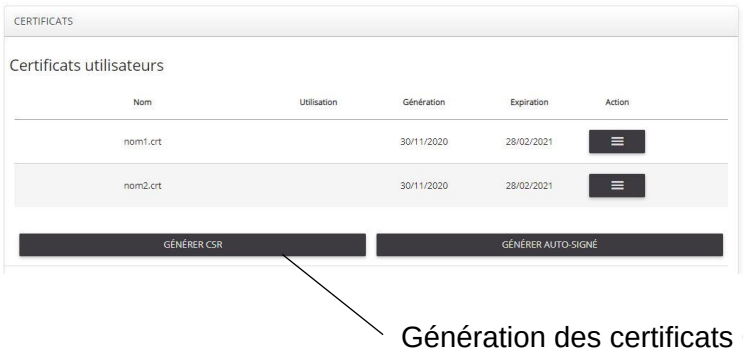
➢ Certificats Signés

Le certificat signé se configure en deux étapes :

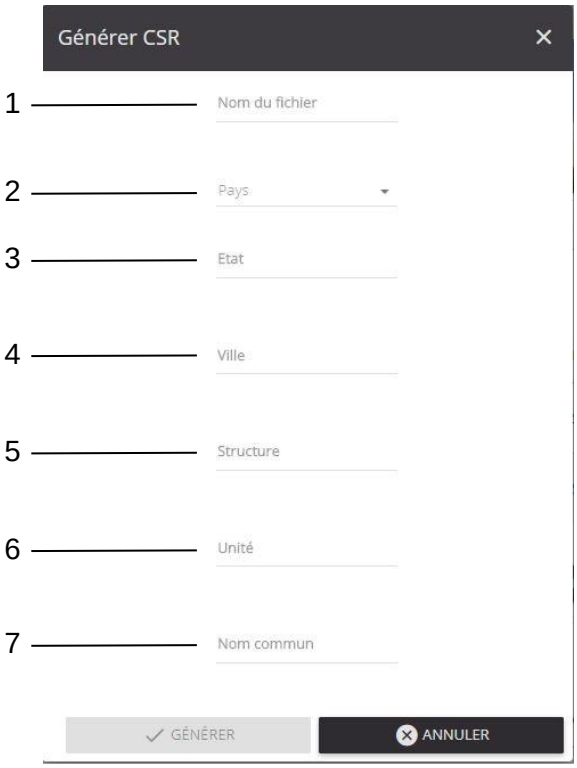
- La première consiste à générer un certificat CSR (de demande de signature) afin de le donner à un organisme d'autorité de certification pour signature.
- La deuxième étape consiste à ré-importer le certificat mais cette fois-ci signé renvoyé par l'organisme d'autorité de certification

Afin de générer le certificat non signé suivre les étapes suivantes :

1. Cliquer sur le bouton « GENERER CSR »



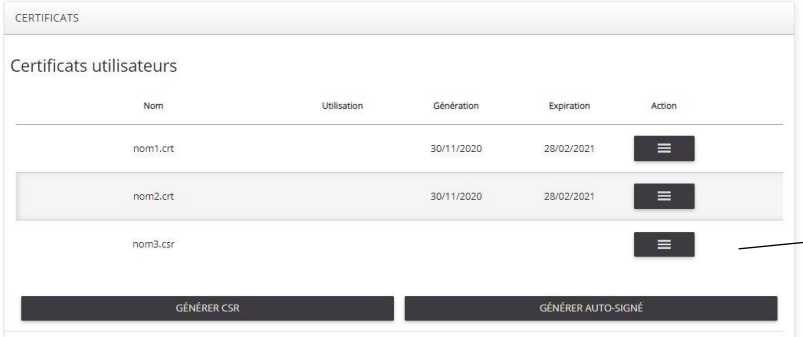
2. Remplir les informations demandées :



1- Nom du fichier : nom qui sera donné au fichier généré
2- Pays : Sélectionner le pays
3- Etat : Correspond à l'état/Région/Département
4- Ville : Correspond à la ville
5- Structure : Correspond à l'entreprise
6- Unité : Correspond au service
7- Nom commun : Correspond à l'adresse IP du concentrateur ou à son nom d'hôte (host name)

Une fois les informations validées, une ligne se crée dans le tableau se trouvant dans la partie « Certificats utilisateurs ». Dans la première colonne on retrouve le nom du fichier que l'on a configuré et dans la dernière colonne l'indication que le certificat est en cours de création.

3. Attendre environ 1 minute pour que le certificat puisse être généré. Pour le télécharger cliquer sur le bouton « Télécharger ».

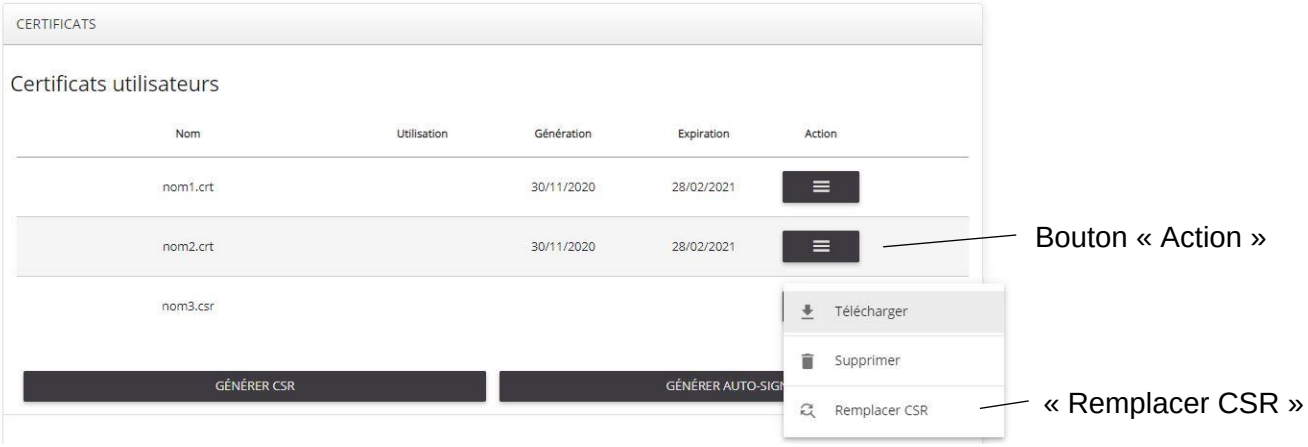


Certificats CSR générés et prêts

Une fois que le certificat CSR a été généré, il est nécessaire de faire signer ce fichier par un organisme d'autorité de certification. Généralement cette étape est réalisée par le RSSI du site.

Une fois cette étape effectuée, et le certificat signé donné par le RSSI, il est nécessaire d'importer ce certificat :

1. Cliquer sur le bouton « Action » de la ligne du certificat CSR puis sur le bouton « Remplacer CSR ».



Le nom du fichier du certificat signé doit obligatoirement avoir le même nom que le certificat CSR

2. Une fois le certificat importé, les colonnes « Génération » et « Expiration » se remplissent.

Le certificat est maintenant prêt à être utilisé, soit dans le paramétrage pour la sécurisation de la page web HTTPS (Configuration / Security), soit pour le paramétrage de la sécurisation de la communication TCP (Configuration / Network).

Une fois le certificat utilisé par une des deux fonctions, la colonne « Utilisation » du tableau sera renseignée.

Pour finaliser le paramétrage d'une communication sécurisée TLS, il est nécessaire d'importer dans le concentrateur le certificat d'autorité racine. Ce certificat (fichier d'extension .crt) est donné par l'organisme d'autorité de certification en même temps que le certificat du concentrateur signé.

➢ CA Certificates

Cette partie permet d'importer des certificats d'autorité racine. Ces certificats sont fournis par un organisme d'autorité racine en même temps que le fichier certificat signé. Il est nécessaire d'importer ce certificat d'autorité racine afin que la communication TLS puisse fonctionner correctement.

Pour importer ce certificat : Cliquer sur « CHARGER » > Sélectionner le fichier certificat > Cliquer sur le bouton « CHARGER ».

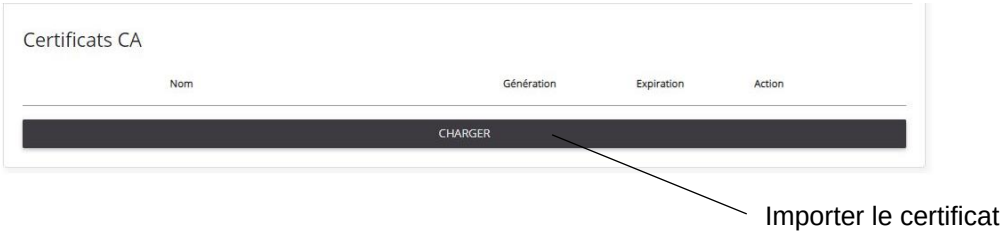
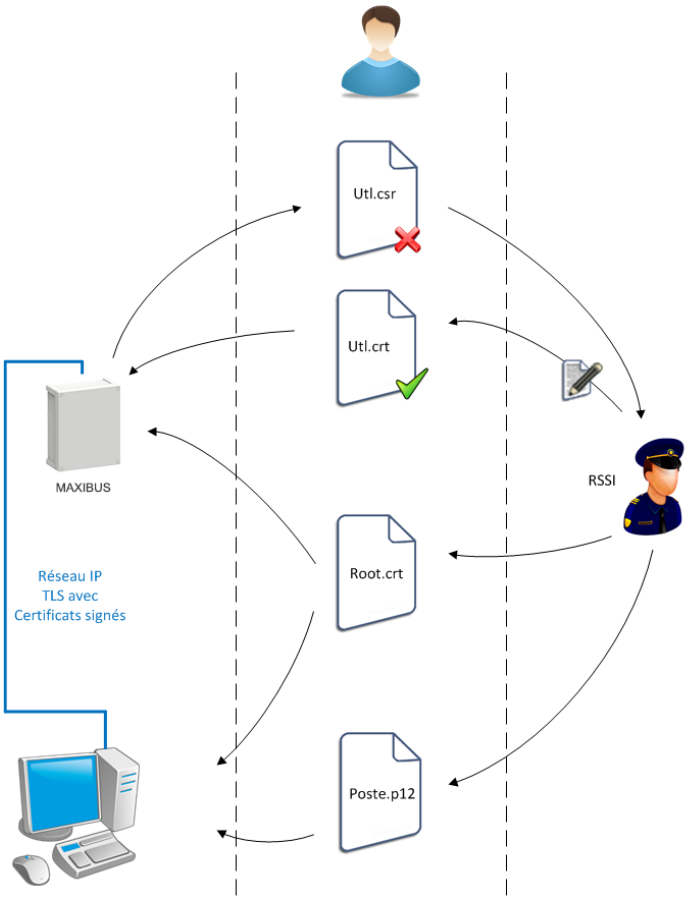


Schéma fonctionnel sur la gestion des certificats pour une communication TLS avec certificats signés :



7.3 802.1X

1. Prérequis :

   Une infrastructure réseau supportant le 802.1X.

   Pour que la sécurité soit active, il faut que l'infrastructure réseau (switch, serveur...) gère le 802.1X

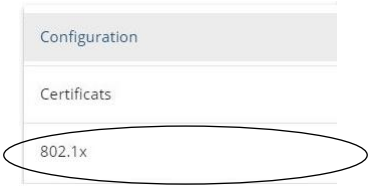
2. Modes et configuration :

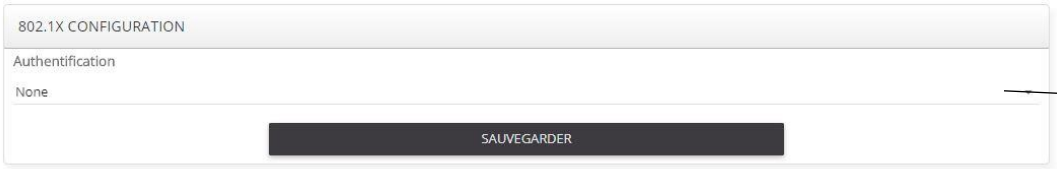
   Veuillez-vous rapprocher de votre Service Informatique pour connaître le type d'authentification utilisé ainsi que les paramètres de connexion.

   Pour les authentifications MD5, MSCHAPV2 et GTC :
   - Le mode EAP (Extensible Authentication Protocol)
   - Anonymous Identity
   - CA Certificate
   - Username
   - Password

   Pour l'authentification TLS :
   - Username
   - CA Certificate
   - User Certificate

Cliquer sur le bouclier puis sur « 802.1X » :

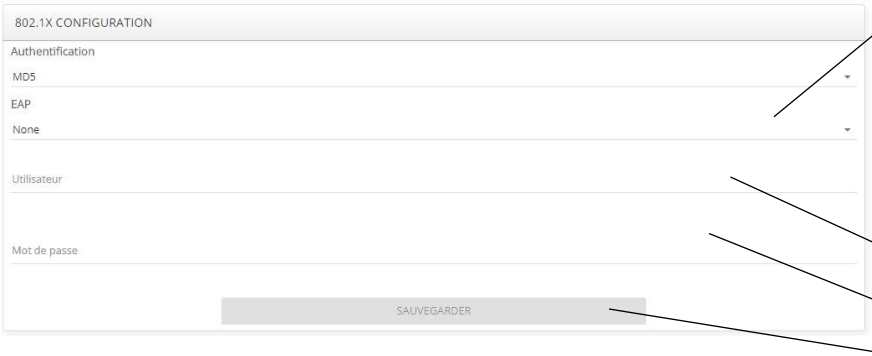




Sélectionner le mode d'authentification

Liste des mode d'authentification :

- Mode « MD5 » :



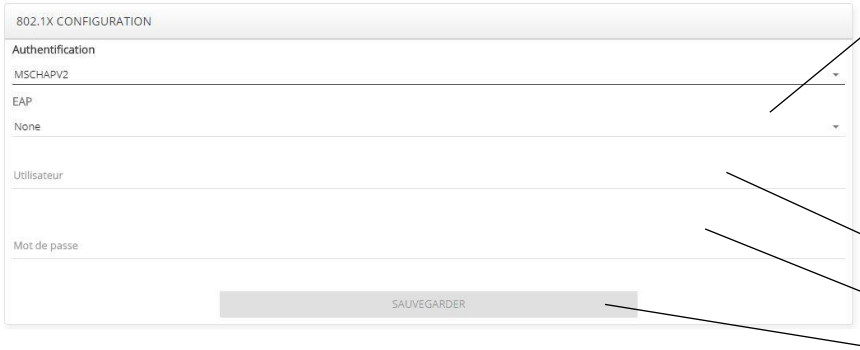
Sélectionner le types d'EAP compatibles :

Sélectionner un nom d'utilisateur

Sélectionner un mot de passe

Sauvegarder les paramètres

- Mode « MSCHAPV2 » :



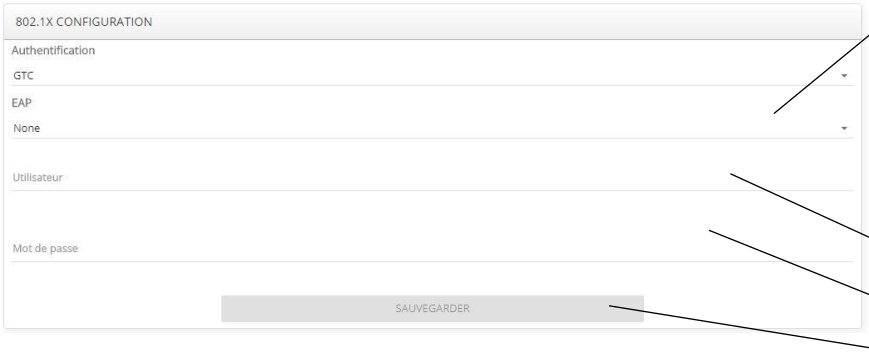
Sélectionner le types d'EAP compatibles :

Sélectionner un nom d'utilisateur

Sélectionner un mot de passe

Sauvegarder les paramètres

- Mode « GTC » :



Sélectionner le types d'EAP compatibles :

Sélectionner un nom d'utilisateur

Sélectionner un mot de passe

Sauvegarder les paramètres

- Mode « TLS » :

Sélectionner un nom d'utilisateur

Sélectionner le type de certificat CA

Sélectionner le certificat utilisateur

Sauvegarder les paramètres

La liste suivante contient les types d'EAP compatibles et les différents modes d'authentification :

- PEAP est une méthode d'authentification 802.1X se servant des certificats des clés publiques sur le serveur afin d'authentifier les clients avec le serveur. L'authentification PEAP génère un lien TLS/SSL crypté entre le client et le serveur d'authentification. Les échanges d'informations sont cryptés et stockés dans ce lien pour assurer que les identifiants des utilisateurs sont sécurisés.

- EAP-GTC (Generic Token Card) est une méthode d'authentification utilisant du texte en clair pour échanger des paramètres d'authentification entre client et serveur. Ce mécanisme d'authentification utilise des tokens utilisables qu'une seule fois (one-time tokens). Cette méthode d'échange d'identifiants est sécurisée.

  EAP-GTC est décrit dans le RFC 2284.

- EAP-MD5 est une méthode d'authentification vérifiant un hash MD5 du mot de passe de l'utilisateur. Cette méthode est fréquemment utilisée dans les réseaux de confiance.

  EAP-MD5 est décrit dans le RFC 2284.

- EAP-TLS (Transport Layer Security) est une méthode d'authentification utilisant une PKI (Public Key Infrastructure) pour la connexion, entre autres, l'authentification d'un serveur RADIUS.
  Cette méthode requiert l'utilisation d'un certificat côté client pour communiquer avec le serveur d'authentification.

  EAP-TLS est décrit dans le RFC 5216.

- EAP-TTLS (Tunneled Transport Layer Security) est une méthode utilisant des certificats côté serveur pour l'authentification entre clients et serveur. Cependant, l'authentification se réalise à l'aide de mots de passe.

  EAP-TTLS est décrit dans le RFC 5281.

- EAP-MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2) est une méthode d'authentification très répandue pour les systèmes MICROSOFT.
  Un serveur RADIUS doit être utilisé comme serveur d'authentification backend.

  EAP-MS-CHAPv2 est décrit dans le RFC 2759.

7.4 HTTPS

L'activation du mode HTTPS se fait depuis le menu configuration après avoir cliqué sur le bouclier .
Pour passer en mode sécurisé, il suffit de cocher la case « HTTPS actif » et de sélectionner un certificat parmi la liste des certificats répertoriés dans le concentrateur (cf. §7.2) :

Une fois le certificat sélectionné, cliquer sur sauvegarder. A partir de là, le concentrateur va rediriger la page vers le mode sécurisé (https://1.2.3.4).

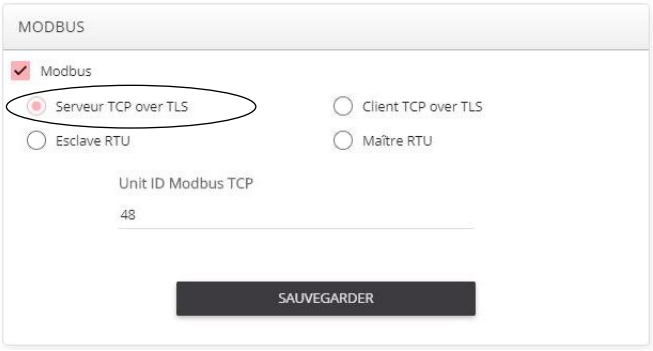
7.5 Modbus chiffré

La sécurisation du ModBus IP passe par la mise en place de tunnels TLS par lesquels vont transiter les données ModBus.
Les tunnels en place utilisent la possibilité de TLS de faire de la redirection de port en encapsulant la donnée dans un tunnel chiffré.

7.5.1 Modbus Serveur chiffré

Pour pouvoir utiliser le chiffrement, activer le serveur TLS du MAXIBUS :

- Dans l'onglet « Concentrateur », Activer le Modbus Serveur TCP over TLS, puis sauvegarder.



- Cliquer sur le bouclier puis sur « Configuration » :

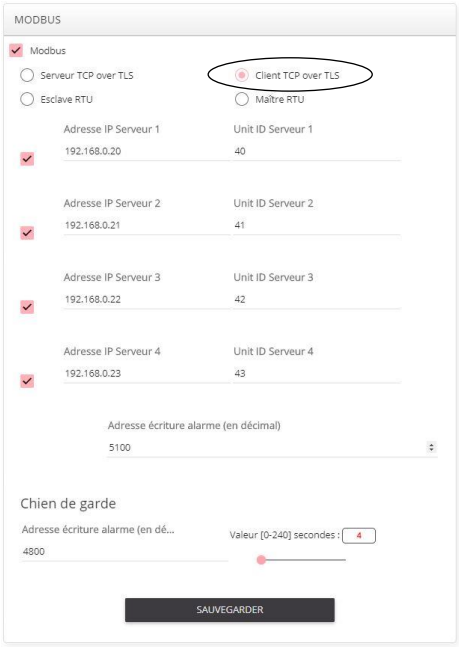
- Activer le « Tunneling TLS du ModBus IP » puis cliquer sur « Sauvegarder ».

Nota : En cas d'activation du tunnel TLS pour sécuriser le ModBus, il est nécessaire pour pouvoir utiliser la cartographie d'activer la gestion de ce tunnel sur le PC client.
En annexe, un exemple de mise en place du chiffrement vers le logiciel de cartographie.
(cf. ANNEXE : Comment activer le Tunneling sur le PC client p.38)

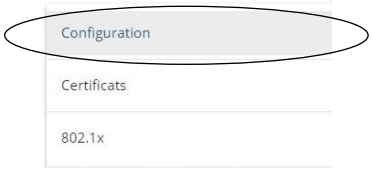
7.5.2 Modbus Client chiffré

Pour chiffrer le Modbus Client, suivre les étapes suivantes :

- Dans l'onglet « Concentrateur », Activer le Modbus Client TCP over TLS, puis sauvegarder.



- Cliquer sur le bouclier puis sur « Configuration » :



- Activer le « Tunneling TLS du ModBus IP » puis cliquer sur « TELECHARGEMENT DE LA CLEF PUBLIQUE DU MAXIBUS ».

Les machines en face du MAXIBUS doivent avoir un serveur TLS.
Placer ce fichier dans les clefs autorisées de TLS.
Par exemple, pour une machine Unix utilisant OpenSSH, la clef récupérée doit être placée dans le fichier « /home/root/.ssh/authorized_keys ».

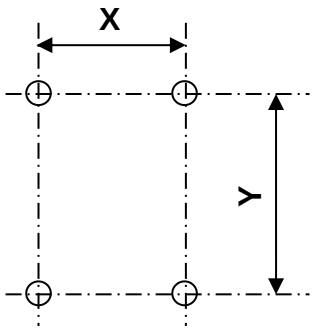
Cliquer sur le bouton « SAUVEGARDER ».

8 CARACTERISTIQUES TECHNIQUES

CARTE CONCENTRATEUR MAXIBUS UNIVERSEL	
• Alimentation	12V DC (10,5 à 14V)
• Consommation max hors alarme	230 mA
• 4 ports COM • Vitesse de communication	liaison RS485 2 fils 9600 bauds
• Liaison pour rapatriement des alarmes • Vitesse de communication • Protocole de communication	RS485 2 fils 9600bds 1 bit start / 8 bits données / 1 bit stop MODBUS RTU
• Liaison pour rapatriement des alarmes • Vitesse de communication • Protocole de communication	Ethernet RJ45 100 Mbits/s MODBUS TCP
• Liaison pour maintenance et paramétrage • Vitesse de communication • Protocole de communication	Ethernet RJ45 100 Mbits/s serveur HTTP
• 8 sorties alarme par contact NF hors alarme	30V AC/DC – 1A
CARTE EXTENSION 8 RELAIS	
• Alimentation	12 V DC (10,5 à 14V)
• Consommation	85 mA
• 8 sorties alarmes par contact NF hors alarme	30V AC/DC – 1A
CARACTERISTIQUES GENERALES CONCENTRATEUR MAXIBUS UNIVERSEL	
• Température de fonctionnement	0°C à + 55°C
• Indice de protection	IP33
• Compatibilité électromagnétique	Conforme aux normes européennes (label **CE**)
• Nombre maximum de relais (maxi 16 cartes extension 8 relais)	136

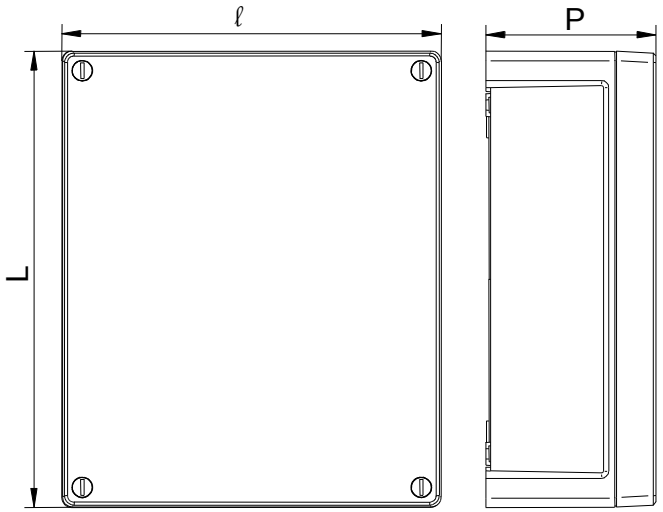
Le gabarit ci-dessous donne les dimensions de perçage du concentrateur MAXIBUS UNIVERSEL avec 1 à 8 cartes extension et du concentrateur MAXIBUS UNIVERSEL avec 9 à 16 cartes extension :

	X	Y
Concentrateur avec 1 à 8 cartes extension 8 relais	188 mm	268 mm
Concentrateur avec 9 à 16 cartes extension 8 relais	360 mm	460 mm
Concentrateur SO-BUS (1 carte extension 8 relais)	163.5 mm	163.5 mm



Dimensions :

Concentrateur MAXIBUS UNIVERSEL



	L	ℓ	P
Concentrateur avec 1 à 8 cartes extension 8 relais	290 mm	240 mm	110 mm
Concentrateur avec 9 à 16 cartes extension 8 relais	500 mm	400 mm	150 mm
Concentrateur SO-BUS (1 carte extension 8 relais)	180 mm	180 mm	100 mm

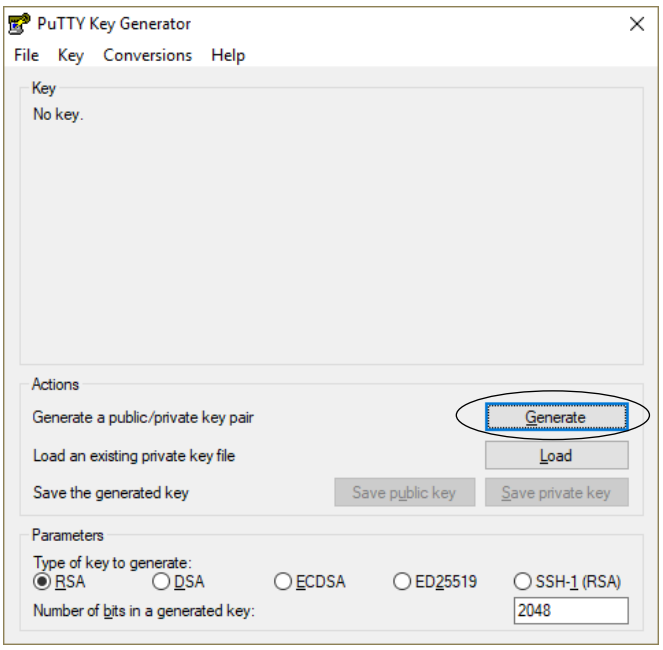
9 REFERENCES DU PRODUIT

- Concentrateur MAXIBUS UNIVERSEL 2 port COM avec 1 à 8 cartes extension réf : 30792001
- Concentrateur MAXIBUS UNIVERSEL 4 port COM avec 1 à 8 cartes extension réf : 30792002
- Concentrateur MAXIBUS UNIVERSEL 2 port COM avec 9 à 16 cartes extension réf : 30792011
- Concentrateur MAXIBUS UNIVERSEL 4 port COM avec 9 à 16 cartes extension réf : 30792012
- Concentrateur SO-BUS 2 COM port avec 1 carte extension réf : 30825000
- Carte extension 8 relais réf : 35588419
- Logiciel de cartographie pour G-FENCE 3000 réf : 38703901
- Carte MAXIBUS UNIVERSEL 2 port COM réf : 80901229
- Carte MAXIBUS UNIVERSEL 4 port COM réf : 80901230
- Kit Carte extension 8 relais réf : 80901218
- Boitier concentrateur vide réf : 80901231

ANNEXE : Comment activer le Tunneling sur le PC client

- **Génération de la clef d'authentification**

Il est tout d'abord nécessaire de créer une paire de clef publique privé en utilisant le logiciel PuTTYgen.

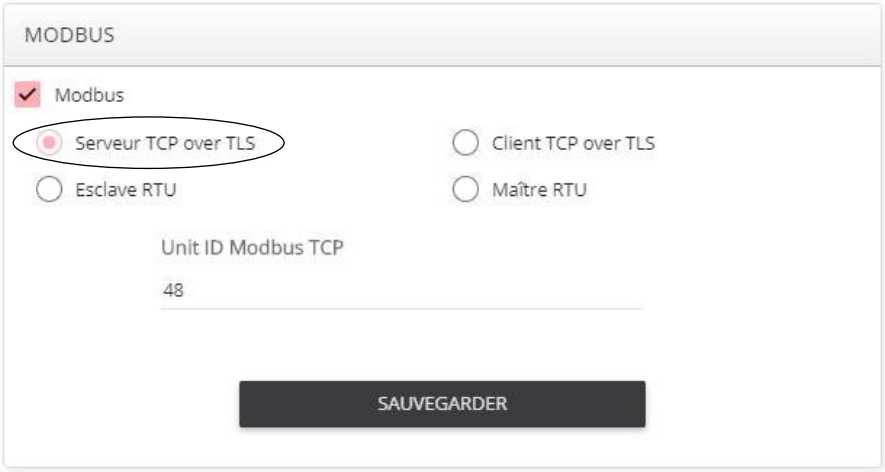


Créer une paire de clef de type RSA puis sauver la clef privée en cliquant sur le bouton « Save private key ».

La clef publique au format SSH est affiché dans le logiciel, la copier-coller dans un fichier (ne pas l'exporter via le bouton « Save public key »).

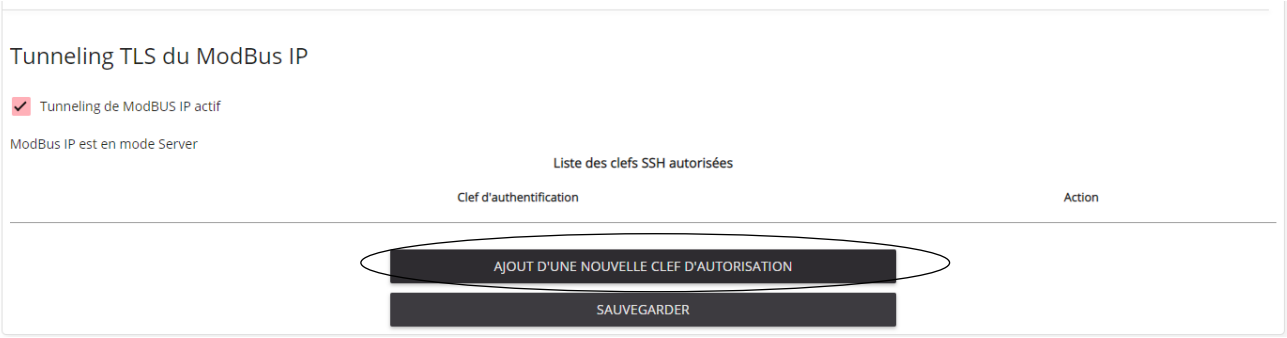
Se connecter au MAXIBUS.

Activer le Modbus Serveur TCP over TLS :



Cliquer sur le bouclier puis sur « Configuration » :

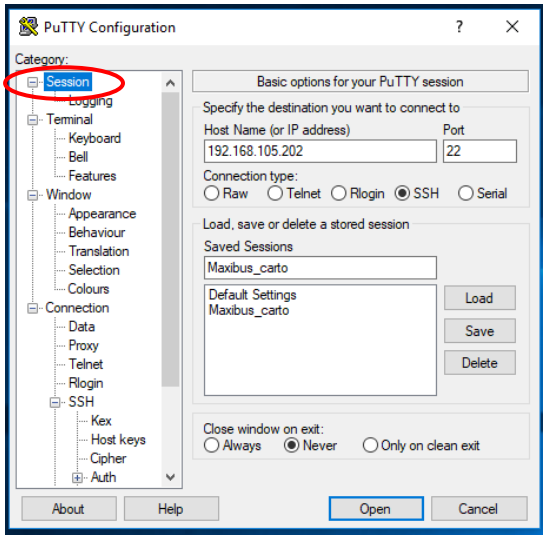
Télécharger le fichier contenant la clef publique dans l'interface Web du MAXIBUS :



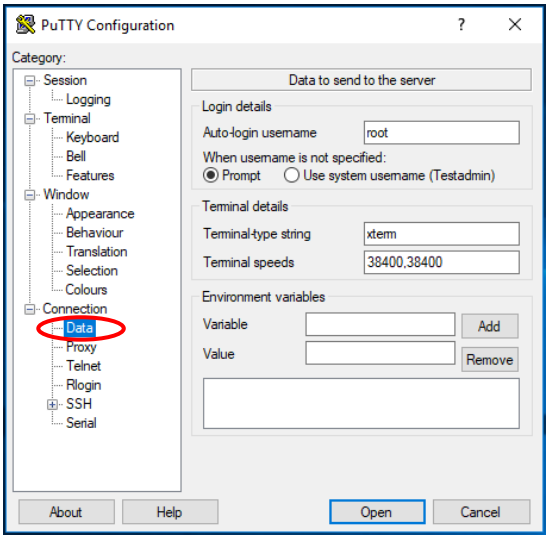
- **Configuration de PuTTY**

Ci-dessous les différents onglets à configurer pour effectuer un tunnel SSH vers le MAXIBUS dont l'adresse IP est en 192.168.105.202 :

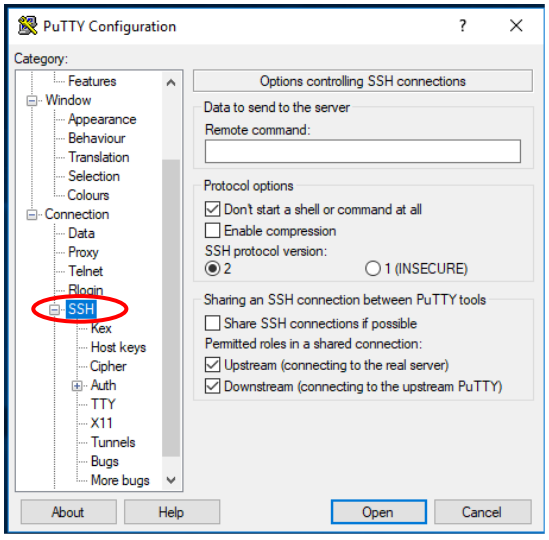
– Onglet « Session »



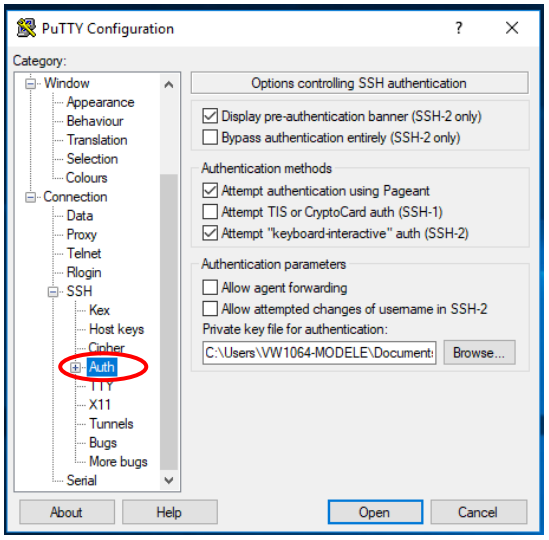
– Onglet « Connection / Data »



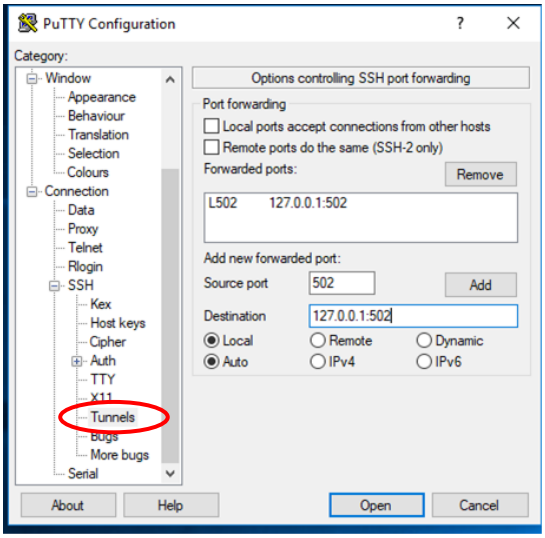
– Onglet « Connection / SSH »



– Onglet « Connection / SSH / Auth ». Entrer la clef privée qui vient d'être sauvegarder. Attention sur certaines versions de Putty les 2 premiers champs sont inversés.



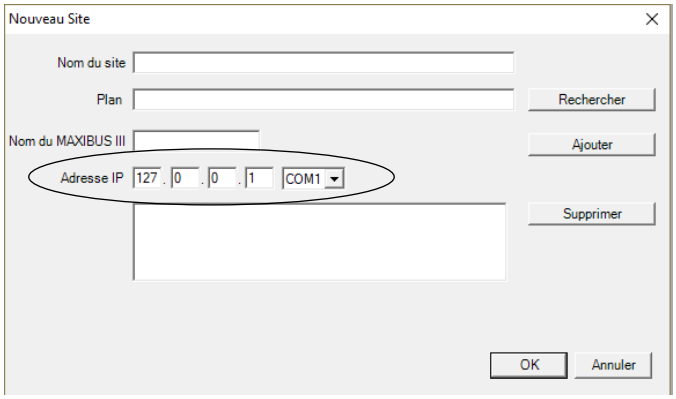
– Onglet « Connection / SSH / Tunnels »



– Cliquer sur « Open »
– Laisser la fenêtre ouverte.

- **Configuration de la cartographie**

Configurer l'adresse du concentrateur en 127.0.0.1



Conformément aux directives européennes sur l'environnement, ce produit ne doit pas être jeté mais recyclé dans une filiale appropriée.

CONTENTS

1 INTRODUCTION

The MAXIBUS UNIVERSAL hub centralizes alarm information pertaining to SORHEA product.

It is composed of a **motherboard** that can manage up to 4 COM ports, 8 alarm contacts. Additional alarm contacts are available via **8-relay extension cards**.

Note: The MAXIBUS UNIVERSAL is for indoor use only.

1.1 Main Features

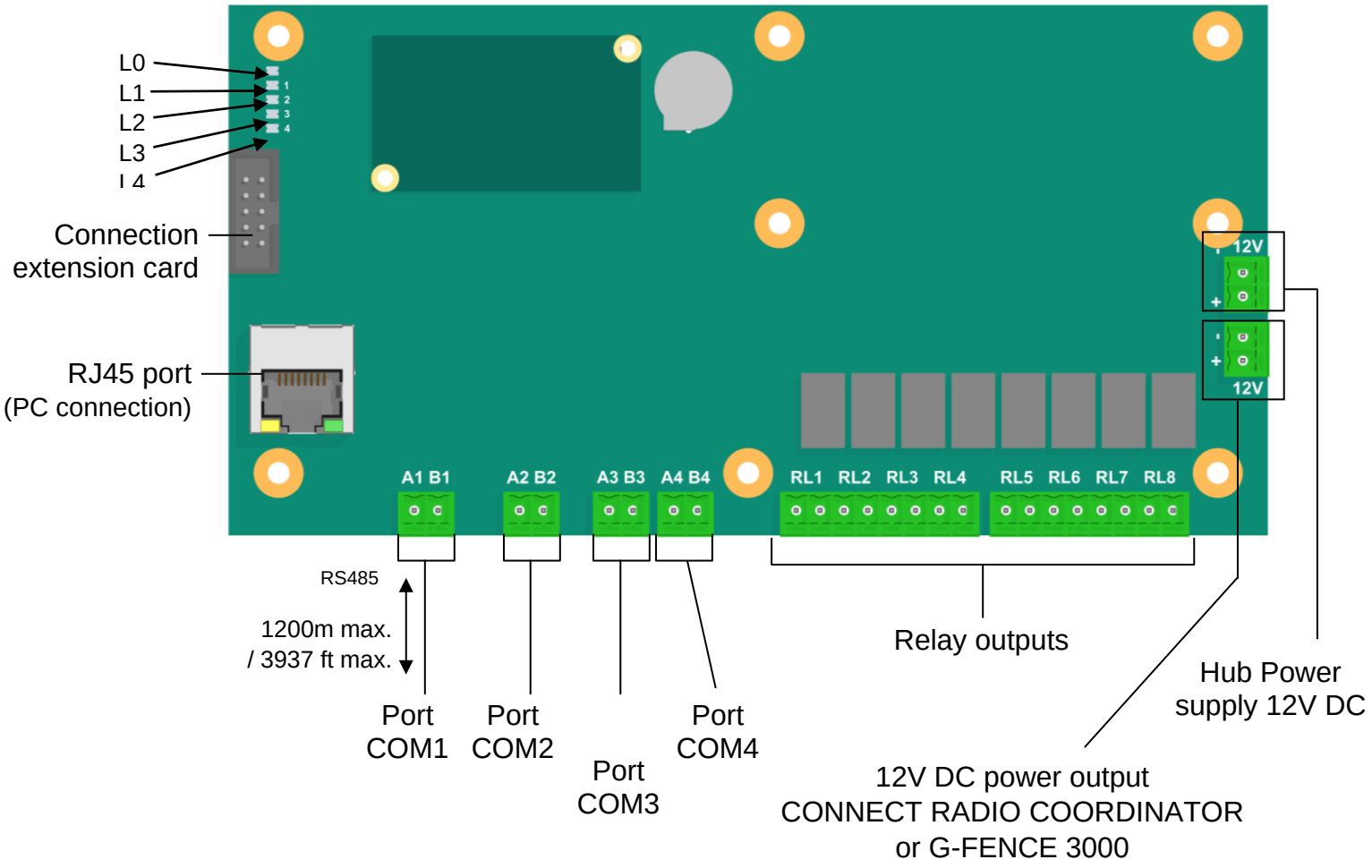
- Centralizes alarm information of all detectors connected to the network.
- Automatic network configuration:
  - Detection of the devices connected to the network
  - Detection of the number of contacts available
- Diagnoses each detector.

1.2 Options

- 8-relay extension card (maximum of 16 extension cards).

2 DESCRIPTION

2.1 MAXIBUS UNIVERSAL hub card

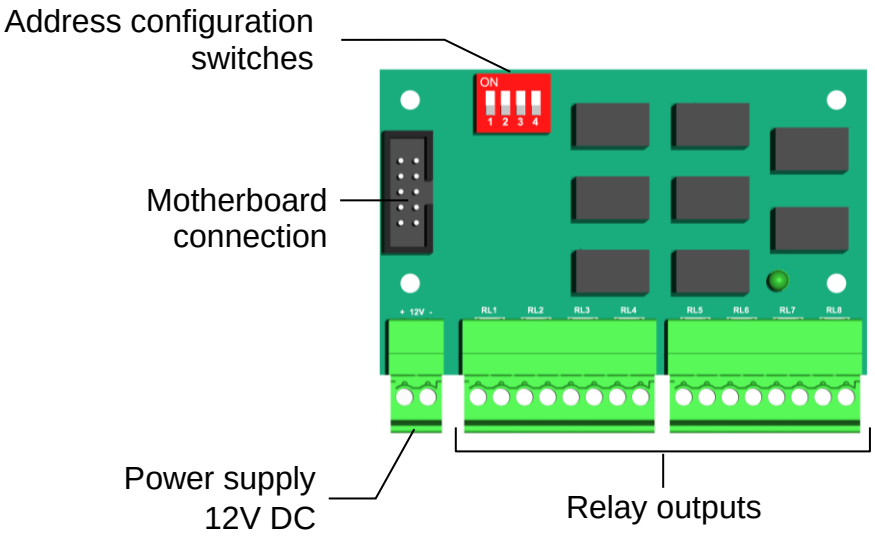


Status of different LEDs:

Status of LED L0 (green)	On	Started
	Off	Offline / startup in progress
Status of LED L1 (red)	Off	Port COM1 of hub not configured
	On	Port COM1 of hub configured
	Blinking	Port COM1 of hub examination in progress
Status of LED L2 (red)	Off	Port COM2 of hub not configured
	On	Port COM2 of hub configured
	Blinking	Port COM2 of hub examination in progress
Status of LED L3 (red)	Off	Port COM3 of hub not configured
	On	Port COM3 of hub configured
	Blinking	Port COM3 of hub examination in progress
Status of LED L4 (red)	Off	Port COM4 of hub not configured
	On	Port COM4 of hub configured
	Blinking	Port COM4 of hub examination in progress

Note: Each COM port can control up to 32 connected network devices.
Each connected product has a unique network address from 1 to 127 per COM port.

2.2 8-relay extension card

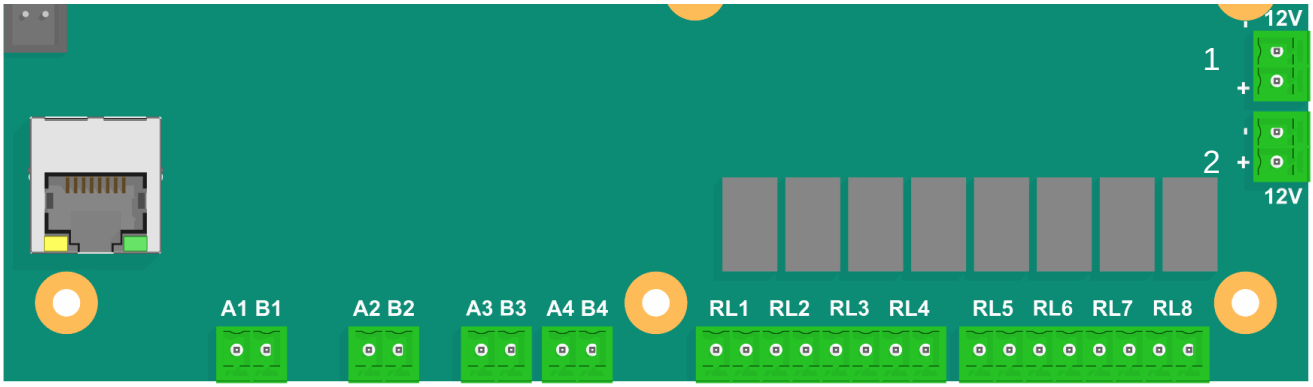


The MAXIBUS UNIVERSAL hub can control up to 16 8-relay extension cards. Each extension card is identified by a fixed number determined by configuration switches as follows:

Position of switches	Address	Position of switches	Address
	1 (OFF OFF OFF OFF)		9 (ON OFF OFF OFF)
	2 (OFF OFF OFF ON)		10 (ON OFF OFF ON)
	3 (OFF OFF ON OFF)		11 (ON OFF ON OFF)
	4 (OFF OFF ON ON)		12 (ON OFF ON ON)
	5 (OFF ON OFF OFF)		13 (ON ON OFF OFF)
	6 (OFF ON OFF ON)		14 (ON ON OFF ON)
	7 (OFF ON ON OFF)		15 (ON ON ON OFF)
	8 (OFF ON ON ON)		16 (ON ON ON ON)

3 CONNECTIONS

3.1 Connections of the MAXIBUS UNIVERSAL hub

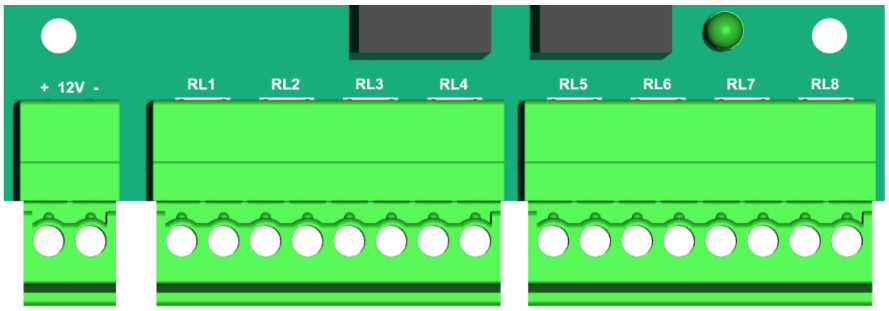


A1	Terminal A bus output RS485 COM1	RL4		Relay contacts 4
B1	Terminal B bus output RS485 COM1	RL4		
A2	Terminal A bus output RS485 COM2	RL5		Relay contacts 5
B2	Terminal B bus output RS485 COM2	RL5		
A3	Terminal A bus output RS485 COM3	RL6		Relay contacts 6
B3	Terminal B bus output RS485 COM3	RL6		
A4	Terminal A bus output RS485 COM4	RL7		Relay contacts 7
B4	Terminal B bus output RS485 COM4	RL7		
RL1	Relay contacts 1	RL8		Relay contacts 8
RL1		RL8		
RL2	Relay contacts 2	1	-	Input power 0V
RL2			+	Input power +12V DC
RL3	Relay contacts 3	2	-	Output 0V port COM
RL3			+	Output +12V DC port COM

The relay contacts are closed when there is no alarm. They are open if alarm or if unaffected or if the MAXIBUS UNIVERSAL hub is switched off. (positive security)

The 12V power supply of the MAXIBUS UNIVERSAL hub shall be equipped with a 2A quick fuse.
It must be grounded to the earth.

3.2 8-relay extension card connections

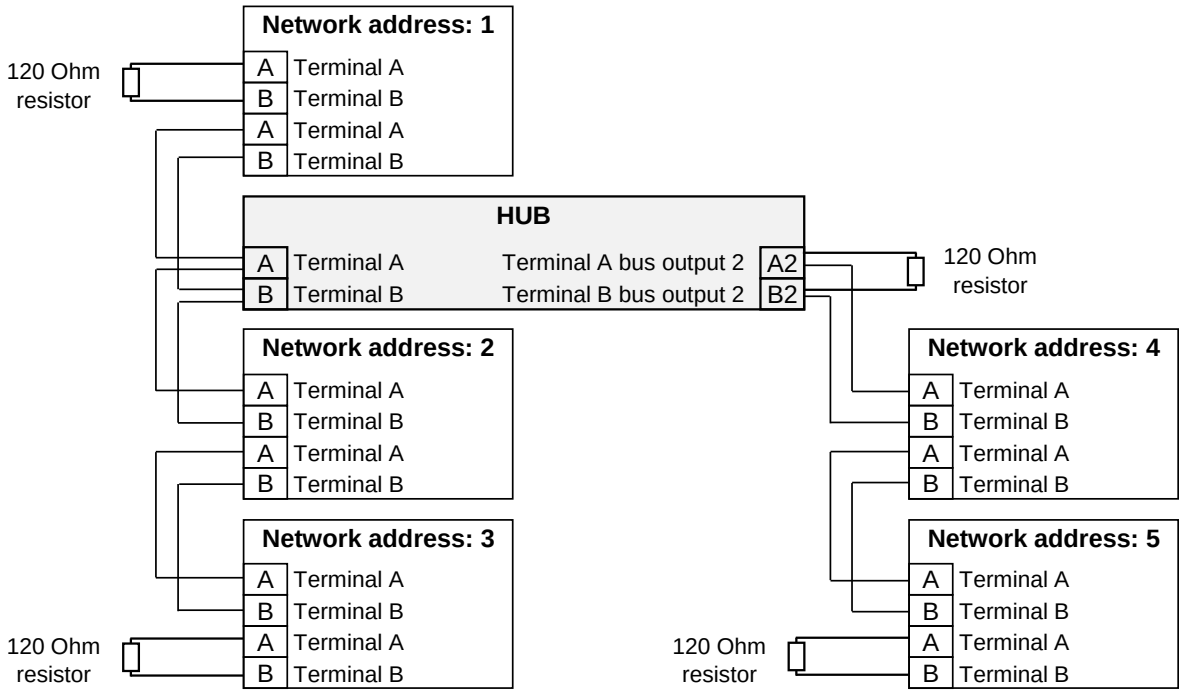


+	Input power + 12V DC	RL5	Relay contacts 5
-	Input power 0V	RL5	
RL1	Relay contacts 1	RL6	Relay contacts 6
RL1		RL6	
RL2	Relay contacts 2	RL7	Relay contacts 7
RL2		RL7	
RL3	Relay contacts 3	RL8	Relay contacts 8
RL3		RL8	
RL4	Relay contacts 4		
RL4			

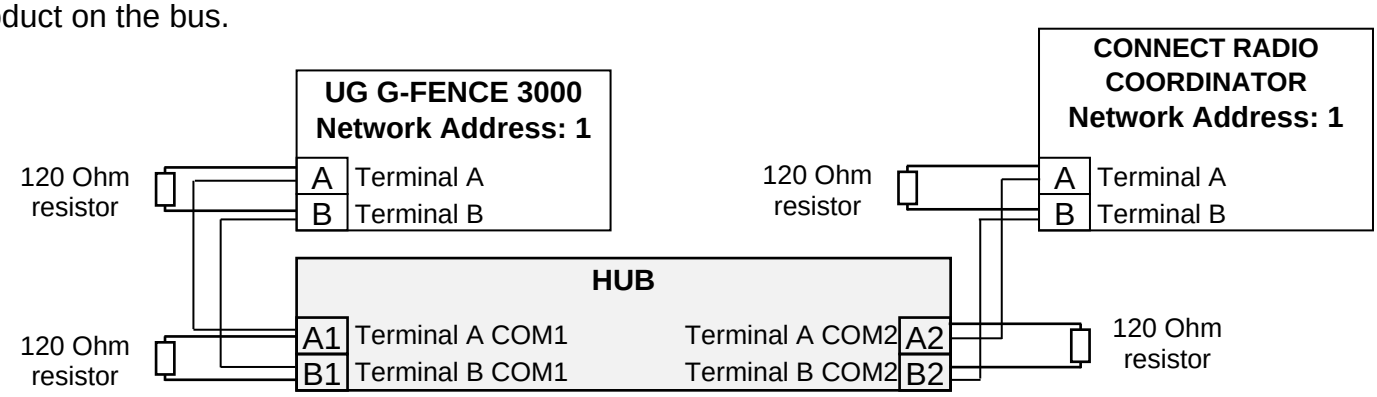
3.3 Wiring to equipment

The networking of products (example: MAXIRIS 3000/3100, PIRAMID CONNECT, CONNECT MODULE…) using the MAXIBUS UNIVERSAL hub forms a serial bus.
It is necessary to connect a 120 Ohm ¼ Watt resistor to both ends of a branch.
A different network address must be assigned to each product connected to the bus (refer to the settings manuals for each product cabled on the bus).
The network addresses must be unique on the same COM port.

Example of products connected to two COM ports:



Note: The G-FENCE 3000 control unit and the CONNECT RADIO COORDINATOR must be alone product on the bus.



4 HUB

4.1 User PC settings

By default, the connection settings of the MAXIBUS UNIVERSAL hub are as follows:

IP address	192.168.105.202
Subnet mask	255.255.255.0

The following procedure allows for the configuration and connection of the user's PC to the column:

Windows* 7 and 8:

- Go to **Control Panel**, double-click on **Network and Sharing Center**, then on the left select **Change adapter settings**, and then click on **Local Area Connection**.
- In the **Networking** tab, Highlight the line **Internet Protocol Version 4 (TCP/IPv4)**, then click **Properties.**
- Choose the option **Use the following IP address** and enter the network settings below.

Windows* 10:

- Go to **Settings**, double-click on **Network & Internet**, then left select **Ethernet**, on the right **Change adapter options**.
- Double-click on **Ethernet**.
- In **Properties**, Highlight the line **Internet Protocol Version 4 (TCP/IPv4)**, then click **Properties.**
- Choose the option **Use the following IP address** and enter the network settings below.

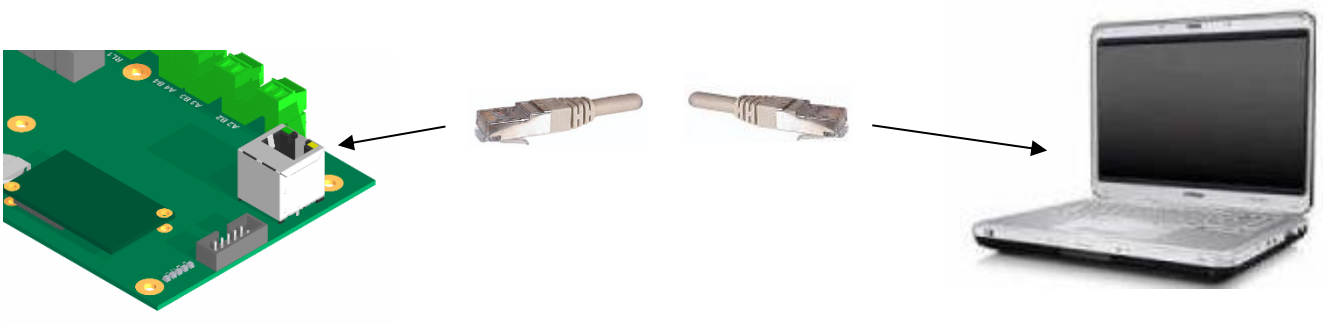
Network settings:

Parameters	**Value**	**Notes**
IP address	192.168.105.XX	The last number must be comprised between 1 and 254 (different from 202)
Subnet mask	255.255.255.0	Mandatory value

* Windows is a registered trademark of Microsoft Corporation

4.2 Connection to the MAXIBUS UNIVERSAL hub

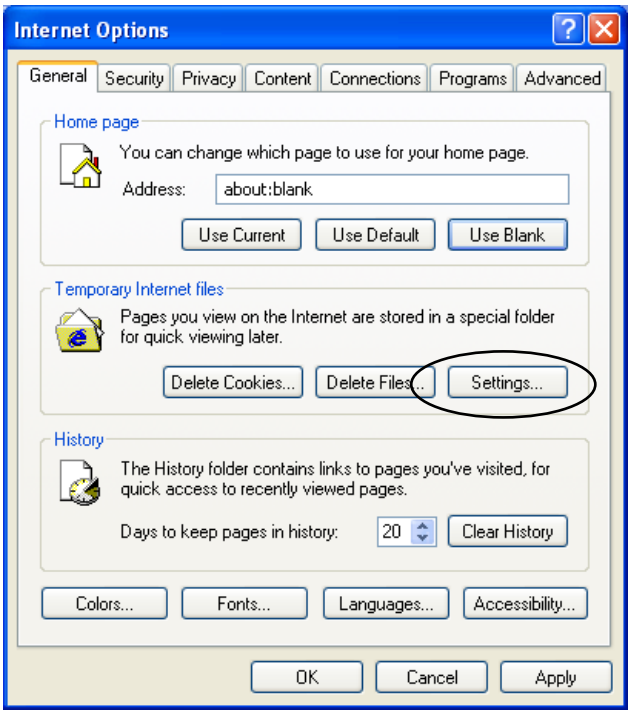
1. Connect the PC to the MAXIBUS UNIVERSAL hub using an RJ45 cable.



2. Open the browser URL.

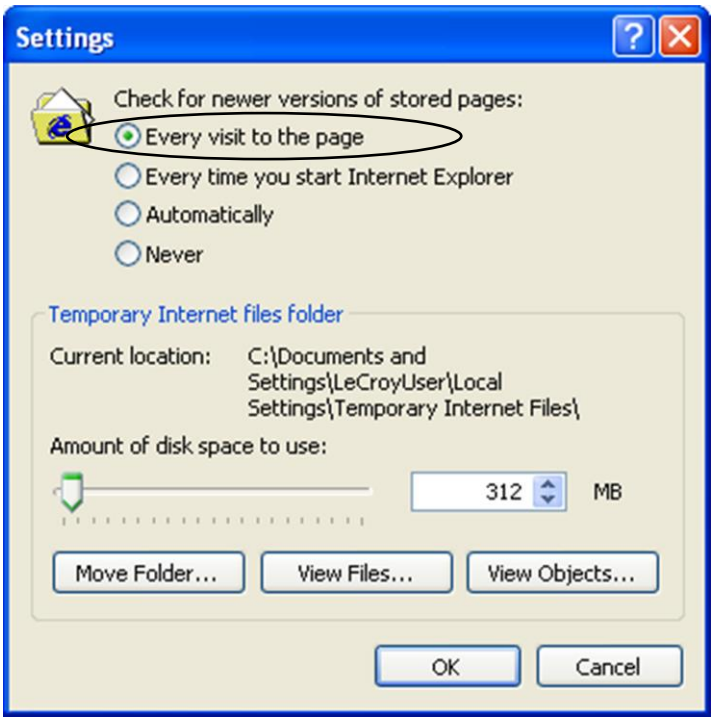
> ⚠ We recommend using Chrome, Firefox and Edge browsers
> The web pages are not compatible with Internet Explorer*

3. Configuration of the browser URL:
   - Choose “**Tools**” in “**Internet Options**”
   - Choose “**General**”
   - In the paragraph “Temporary Internet files”, click on “**Settings**”

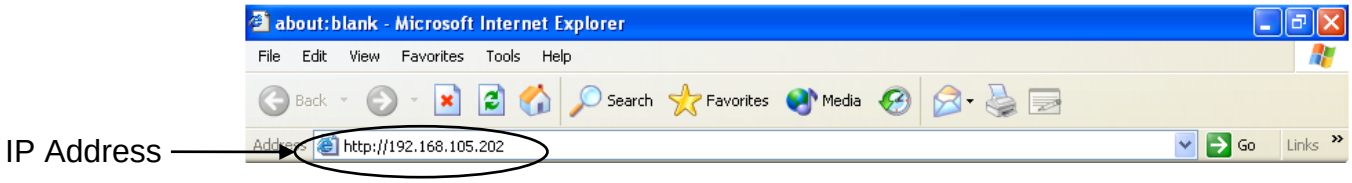


* Internet explorer is a registered trademark of Microsoft Corporation

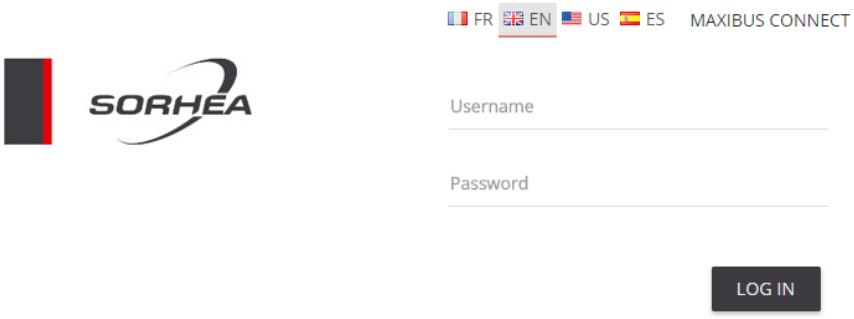
– Check that the parameter "***Every visit to the page***" is validated (activated).



4. Enter the IP address of the MAXIBUS UNIVERSAL hub into the browser URL. (by default: **192.168.105.202**)



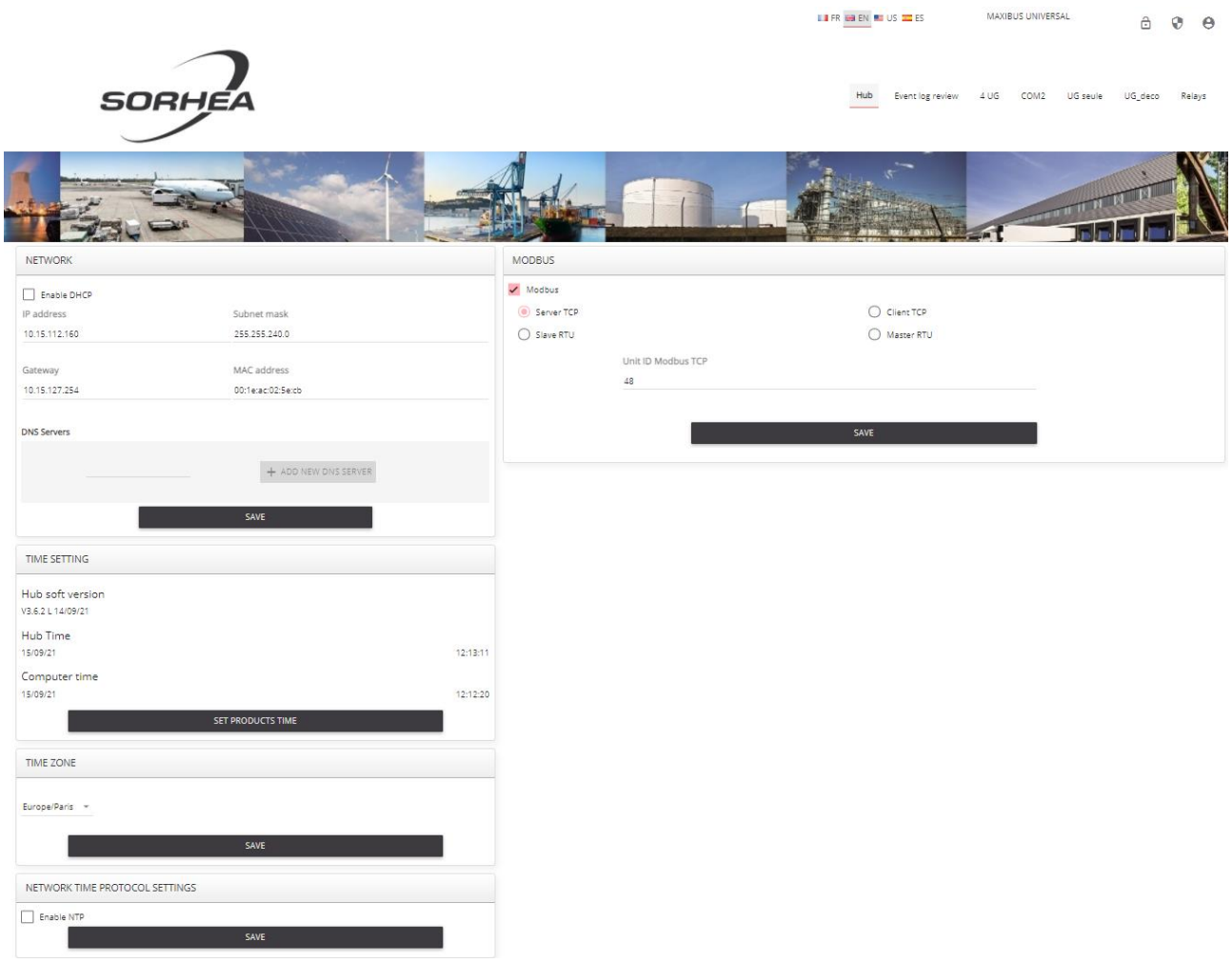
5. Enter login and password (managing 2 connection levels):



Access type: Read only access	
Login	user
Password	0000
Access type: Read and write access	
Login	admin
Password	␣␣␣␣(4 spaces)

Once the password is validated, all tabs of the web server are available and let you switch between the different MAXIBUS UNIVERSAL hub features.

Home page:

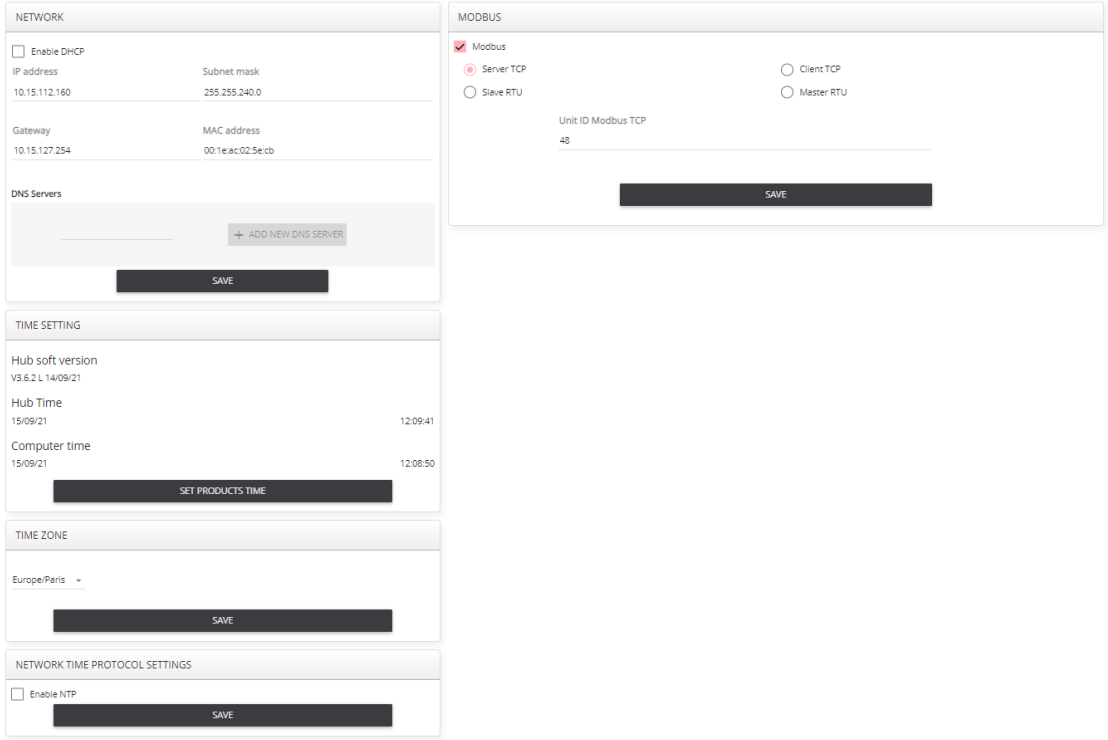


4.3 Change settings for the MAXIBUS UNIVERSAL hub

Note: To change settings for the MAXIBUS UNIVERSAL hub, you need to connect as **admin**.

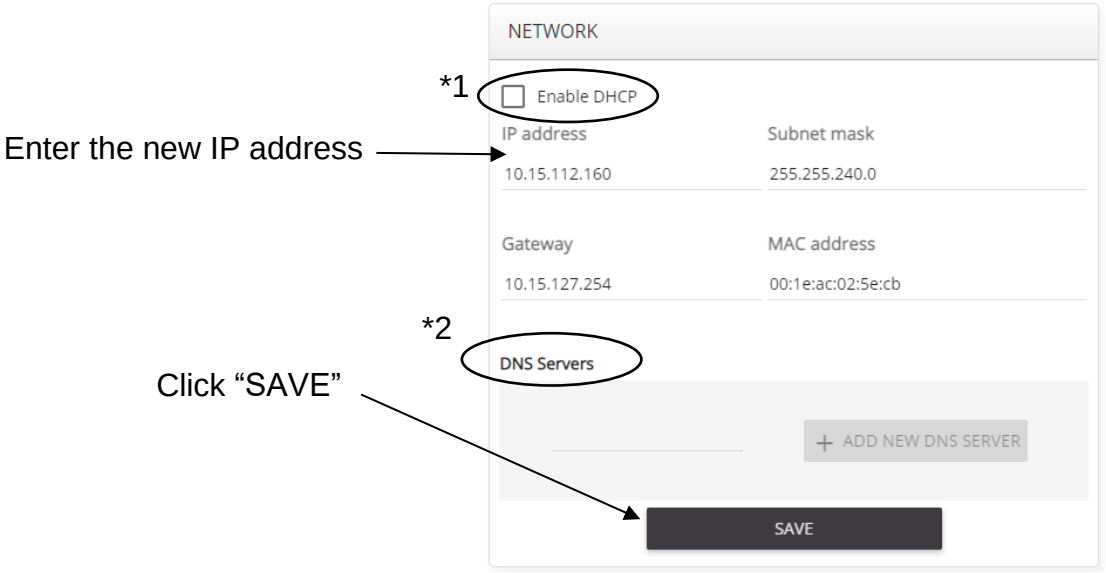
Network configuration (see §4.3.1)

Setting the time (see §4.3.2)



4.3.1 Networks settings

1. Change the selected setting then click “**SAVE**”.



2. Wait for the refresh of the page to the new IP address.

1 DHCP configuration:

The MAXIBUS automatically retrieve a new IP address from the DHCP server. The redirection to the new web page won’t be automatic, the user must retrieve the new IP with the network administrator. Once the new IP is found, the user will see a green dot on the web page to indicate that the DHCP is functional. If the dot is red, it means that the MAXIBUS wasn’t able to retrieve a new IP from the DHCP server.

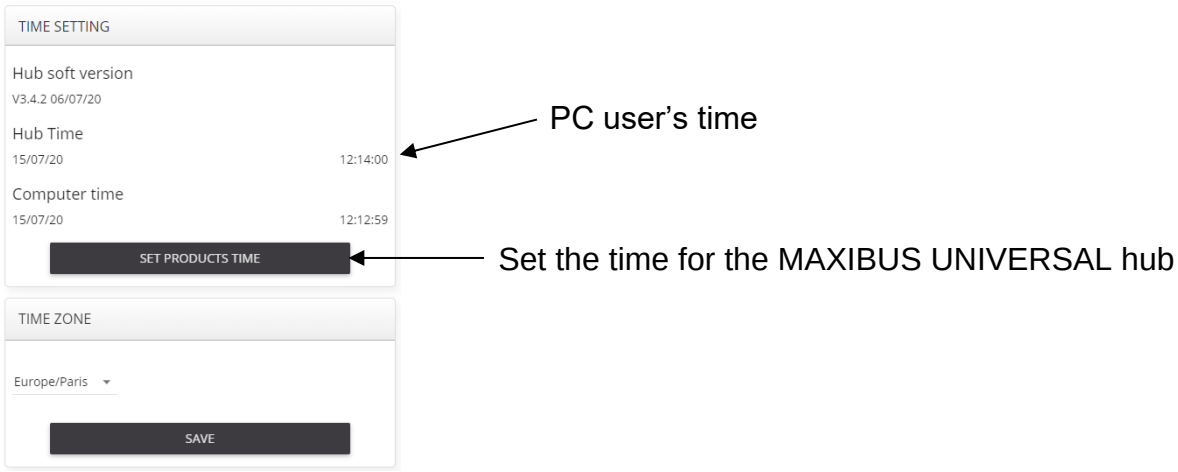
2 DNS Server configuration:

The user can configure one (or two) DNS server on the MAXIBUS. For now, the DNS functionalities are limited to NTP server configuration using a domain name instead of an IP address (refer to part 4.3.2).

4.3.2 Setting the time on the MAXIBUS UNIVERSAL hub

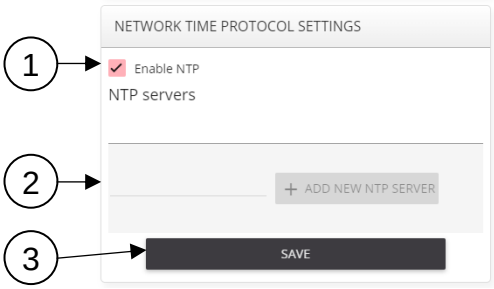
Manual time setting:

Select “**SET PRODUCTS TIME**” to set and coordinate the time of the hub with the time of the PC user.



Automatic time setting by NTP:

It is possible to synchronize the time of the MAXIBUS on time servers.
This synchronization uses the NTP protocol.



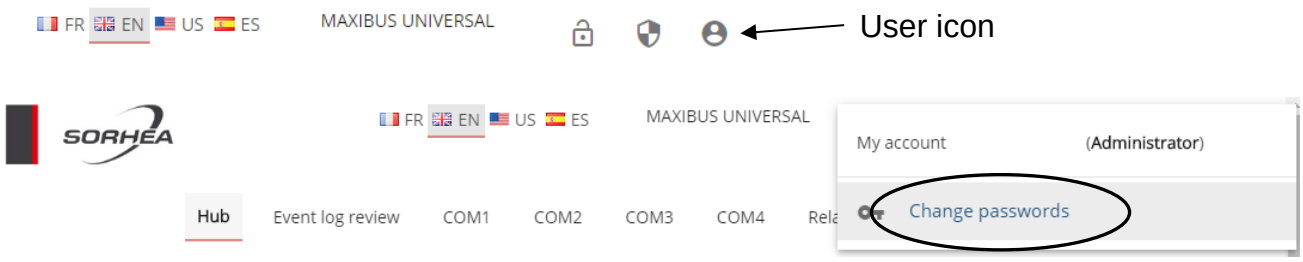
1. Click on the box to activate the NTP.
2. Add the IP address of the NTP server and click on "+ ADD NEW NTP SERVER".
3. Click on "Save".

Note:

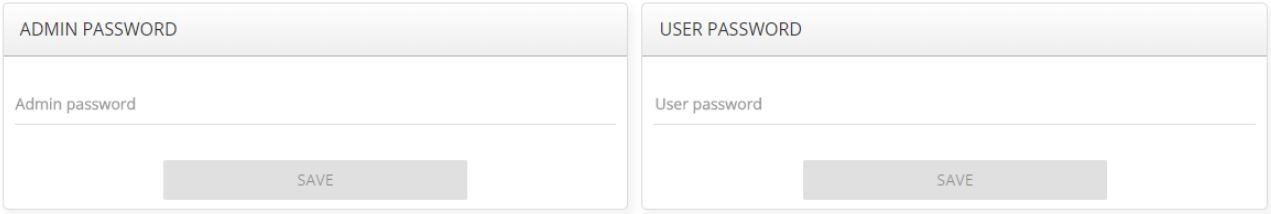
NTP can be activated by using a server IP address or its domain name. Adding a NTP server with domain name require to firstly activate a DNS server (refer to part 4.3.1).

4.3.3 Change passwords

1. Select the user icon in the top right corner and choose “**Change passwords**”



2. Enter the new Administrator password for the login “**ADMIN”** or the new User password for the “**USER”** login and confirm with “**SAVE”**.



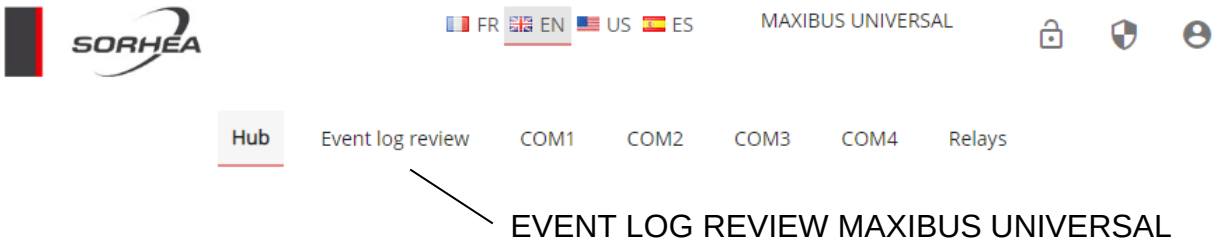
Note: the password can contain up to 30 characters.

3. Wait for the page to refresh, then choose “**HUB**” to return to the home page.

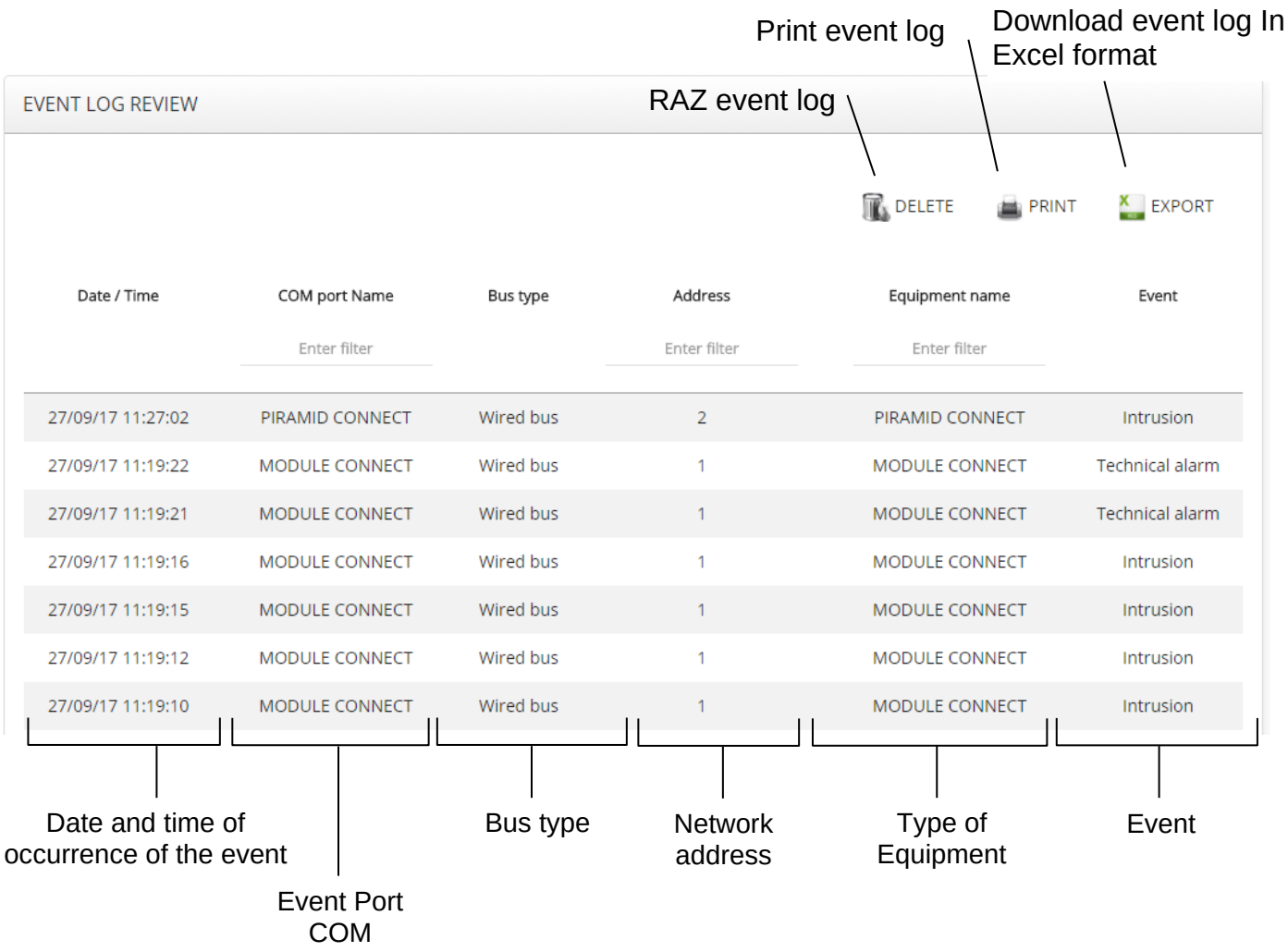
4.4 Viewing the event log of the MAXIBUS UNIVERSAL HUB

This log displays the event history for the whole site.
Only technical and intrusion alarms occurred on the connected devices and changes to the hub's configuration are displayed.

Click the "Event log review" tab.



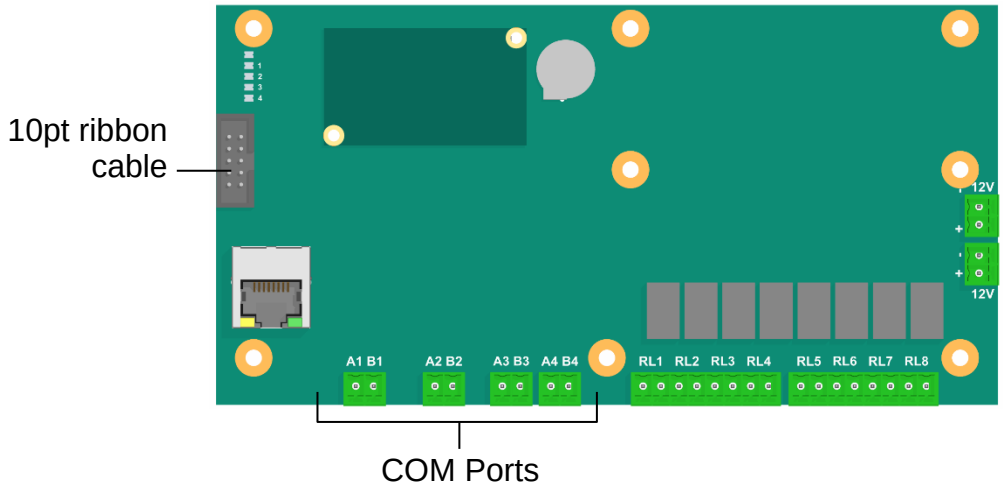
Event log detail:



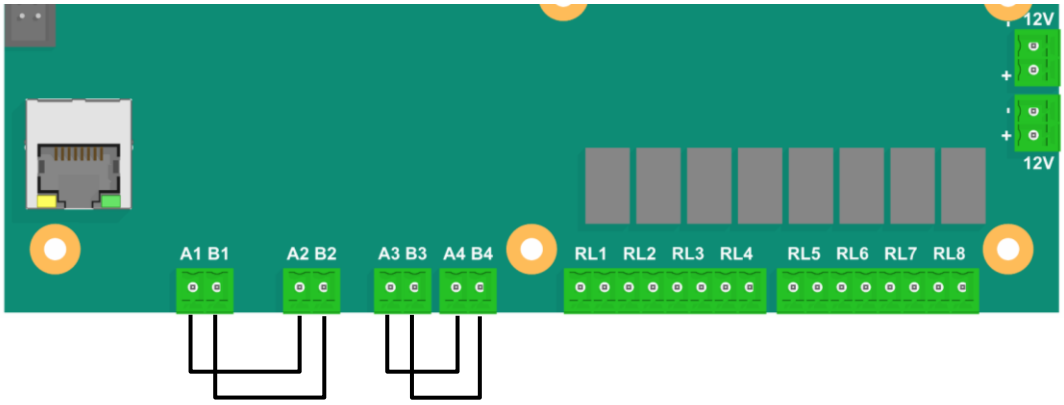
4.5 Reset procedure for the MAXIBUS UNIVERSAL hub IP Address

If the MAXIBUS UNIVERSAL hub IP address modified by the user is lost, the following procedure will give you a factory reset of the IP address.

1. Power off the MAXIBUS UNIVERSAL hub.
2. Unplug all COM ports connected.
   Unplug the 10pt ribbon cable between the MAXIBUS UNIVERSAL hub and the 8 relays extension cards.
   Disconnect the RJ45 connector and the relays.



3. Follow the wiring diagram as shown on the below picture:



4. Turn the MAXIBUS UNIVERSAL hub power on and wait for the following sequence:

   The green light L0 is lit and stable.
   The L1 to L4 lights are on a LED chaser mode.

5. Unplug the wiring done on step 3 and wait for the LED chaser to end

6. Reconnect the RJ45 connector and log on to http://192.168.105.202/

7. Plug in the connected COM ports.
   Replug the 10pt ribbon cable between MAXIBUS UNIVERSAL hub and the 8 relays extension cards.
   Replug the relays.

8. Do an update of the date and time. (see §4.3.2)

4.6 Replacement procedure of the memoire cell

The memory cell has an average lifetime of **10 years**.

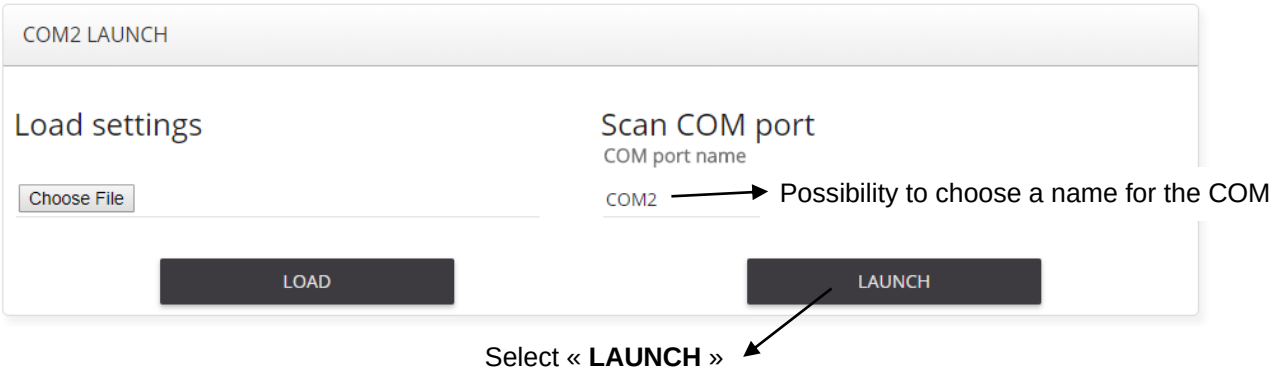
Make a backup of the configuration of the site and the relay settings when commissioning is finished. (See §5.4.1)
When the memory cell is low, replace the MAXIBUS UNIVERSAL hub electronic board and upload the configuration of the site and the relays. (See §5.4.2)

5 MANAGING THE COM PORTS

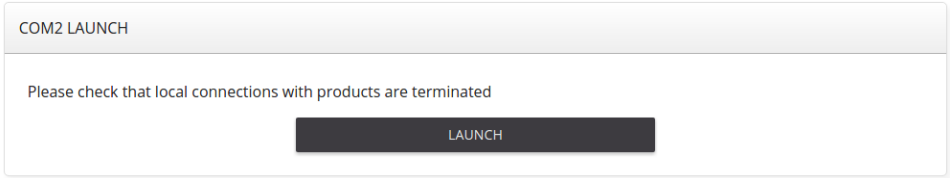
5.1 Configuration of the COM port

1. Click the COM port to be configured.

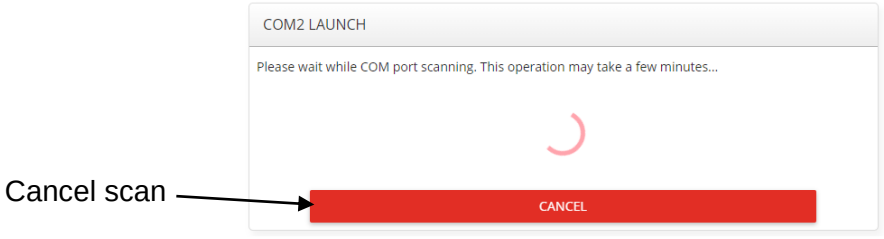
2. Click “LAUNCH” to start configuring the COM port.
   Note: it is possible to choose a name for the COM port (by default, the name of the COM port is the type of product)



3. Please check that local connection with products are terminated : unplug the RJ45 link, close the smartphone application. Click “LAUNCH”.

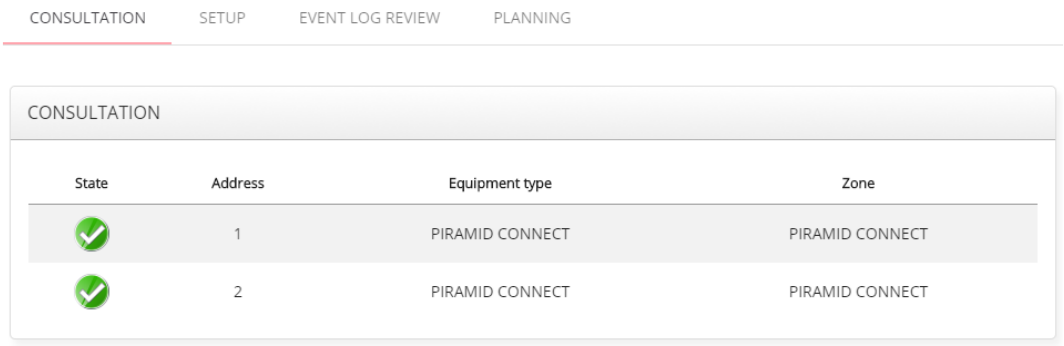


4. Wait for the configuration page to load.
   Waiting while scanning.



5. The devices found are displayed in a list.
   For user instructions please consult the device manual.

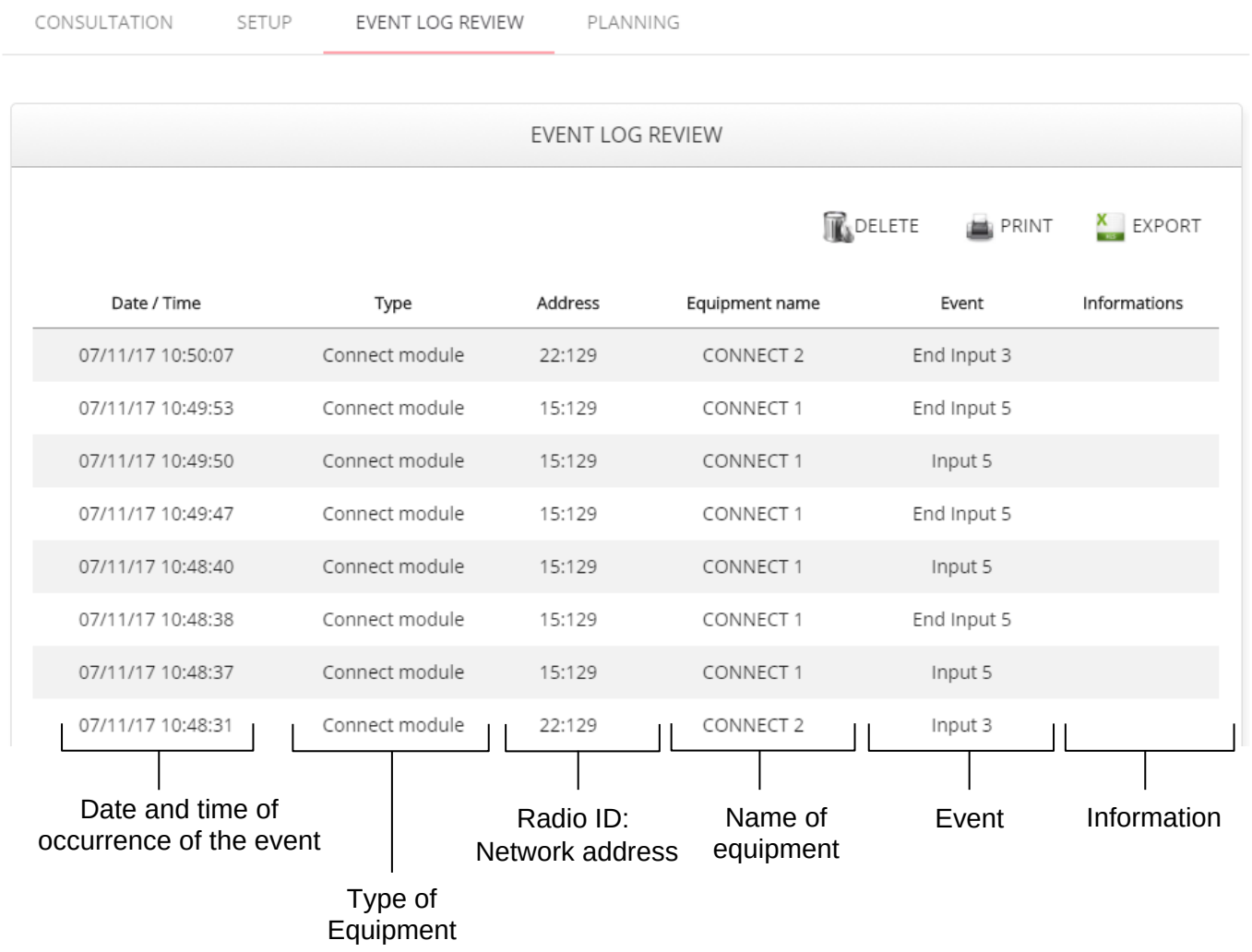
Example of the screen at the end of the search:



5.2 Event Log port COM

This is a concise event log for the COM port.

Log event example:



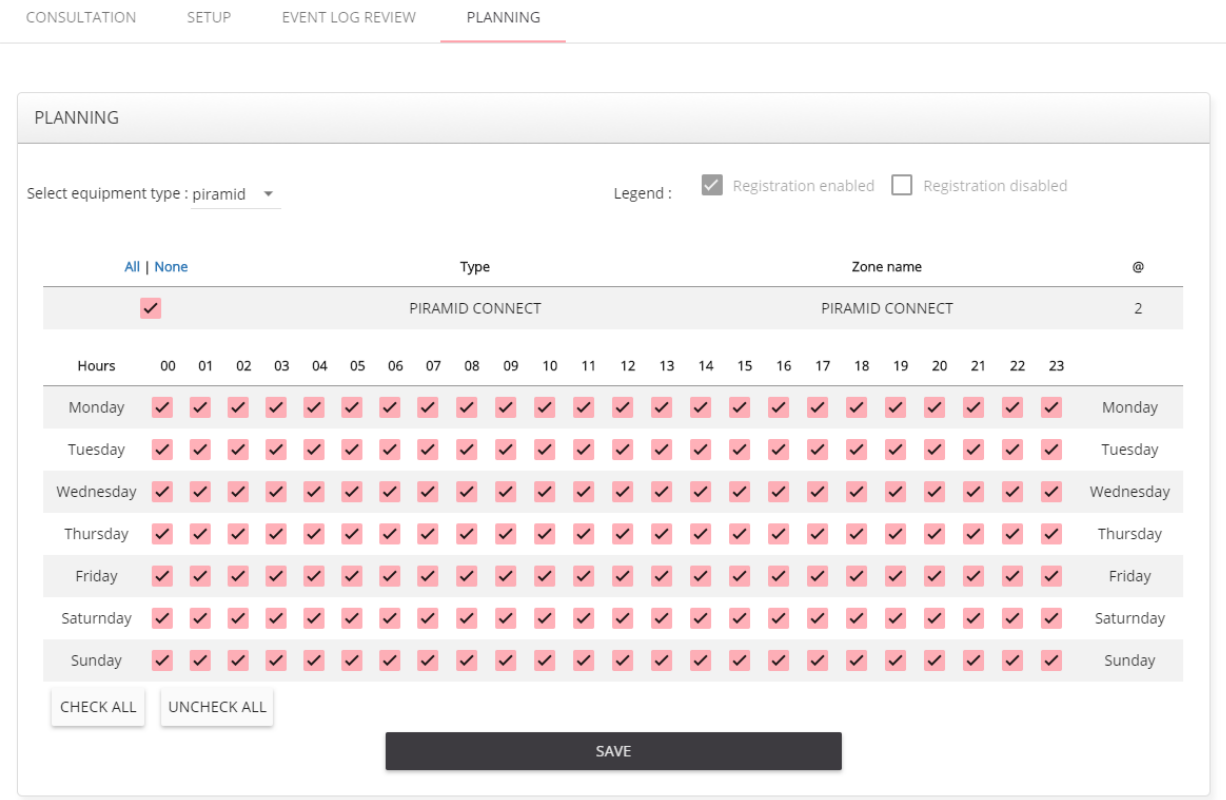
5.3 Managing the history schedule

The objective is to avoid saving of alarms selected in the log. However, the alarm outputs remain active.

Note: by default, all alarms of devices connected to the MAXIBUS UNIVERSAL hub are stored in event log.

- Go to the COM port for which a schedule must be configured.
- Select "**PLANNING**".
- By default, all devices are checked.

1. Choose the device for which a schedule must be specified.
2. Select the periods of registration and non-registration for the element.
3. Select "**SAVE**".



Note: for unchecked devices are permanently stored.

5.4 Saving and loading the settings of a COM port

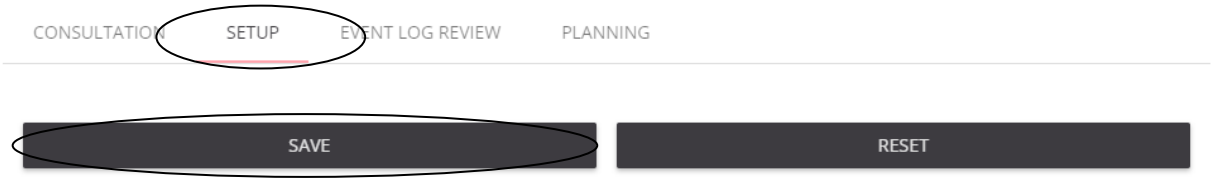
Each COM port of the MAXIBUS UNIVERSAL hub can be saved independently.
The MAXIBUS UNIVERSAL hub stores:

1. The COM port settings
2. The assignment of the COM port's relays
3. The site configuration linked to the COM port

It is possible to backup these settings on the MAXIBUS UNIVERSAL hub and to restore them.

5.4.1 Saving the MAXIBUS UNIVERSAL hub settings

- Go to the COM port to be saved.
- Select “**SETUP**”, then “**SAVE**”.

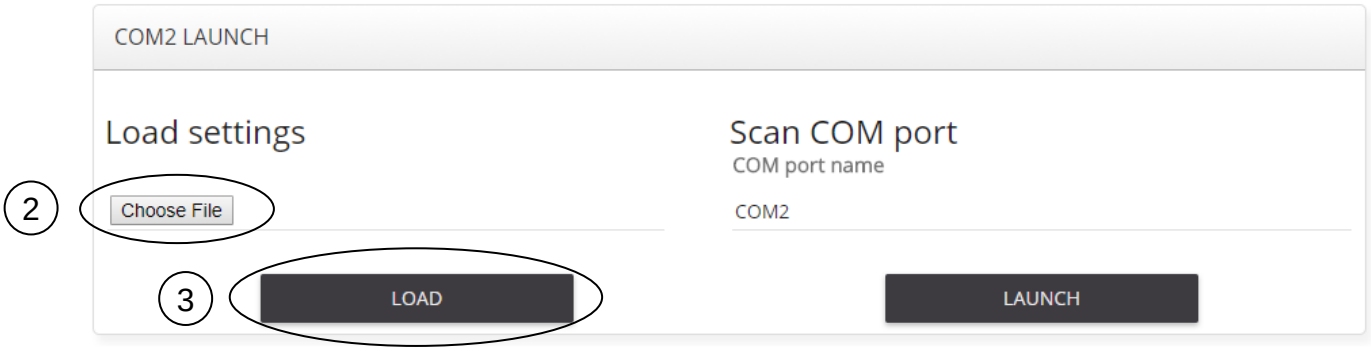


- The file NETWORKx.conf (x = number of COM port) is loaded.

5.4.2 Loading the configuration to the MAXIBUS UNIVERSAL hub

Note: to load the configuration of a COM port, it needs to have been reset to zero.
(See §5.5 Resetting a COM port)

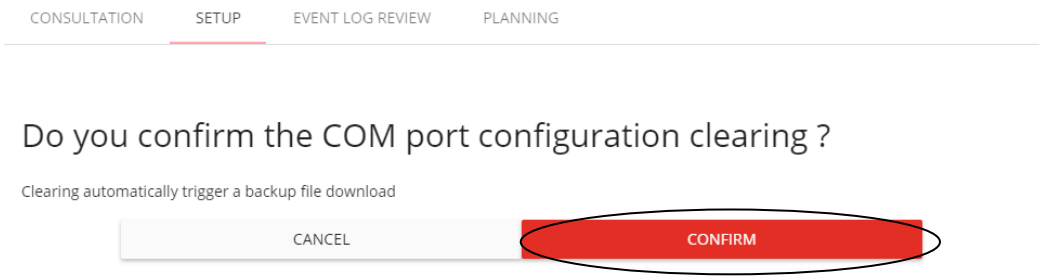
1. Click the COM port to be configured.
2. Choose the file to load.
3. Click the LOAD button.



5.5 Resetting a COM port

- Go to COM port to reset.
- Select “**SETUP**”, then “**RESET**”.

- Confirm reset of COM port.

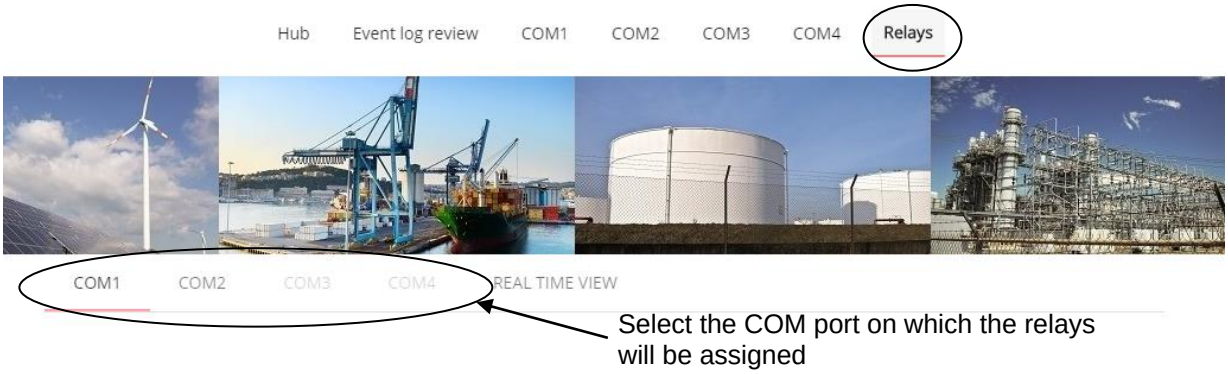


6 MANAGING ALARM OUTPUTS

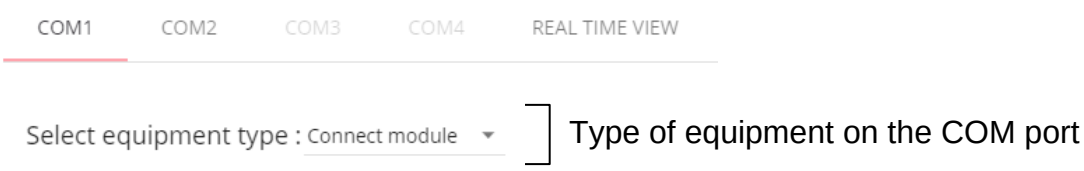
6.1 Assignment of relay outputs

<u>Process to associate the relays</u>:

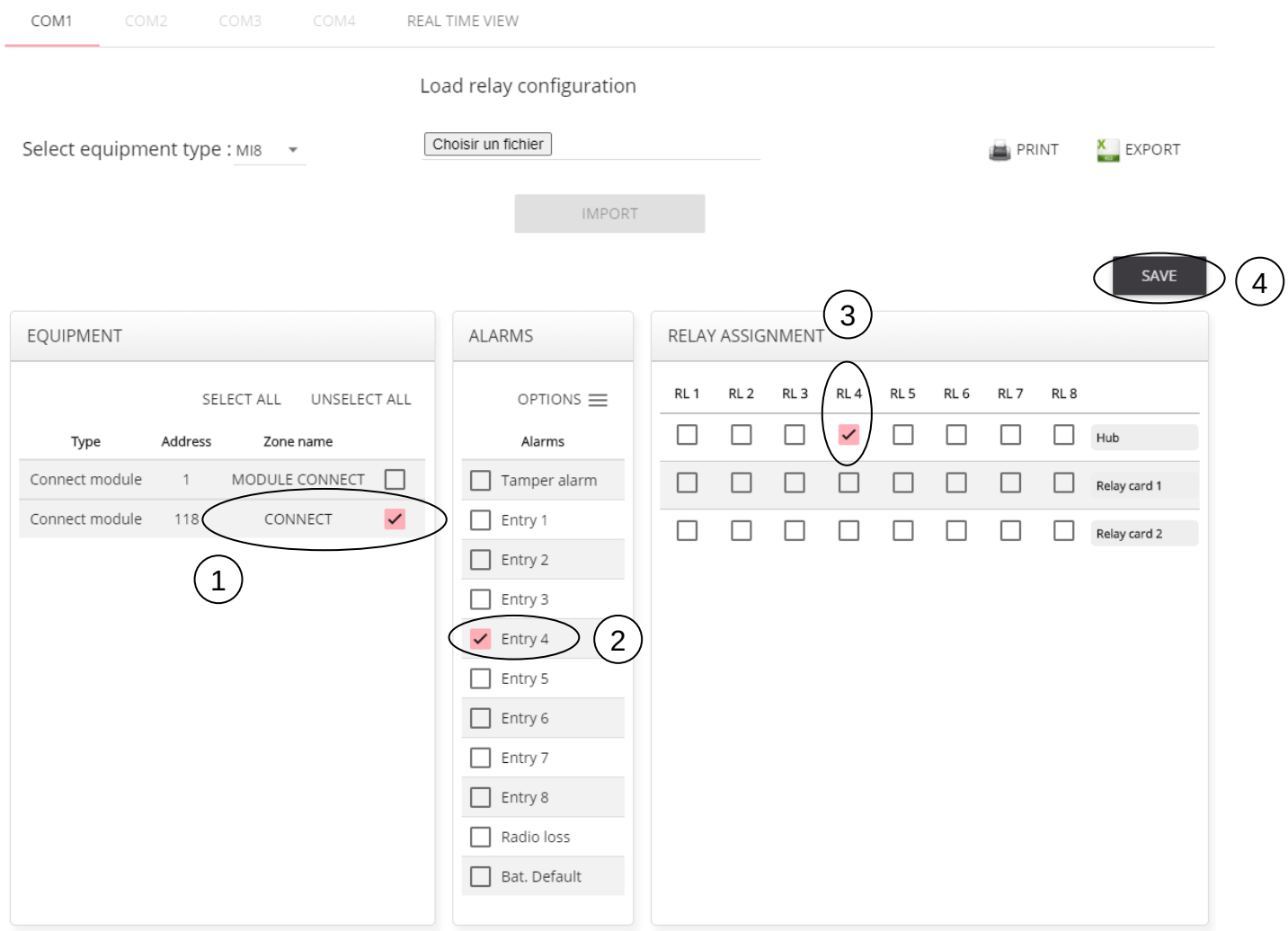
- Choose “**Relays**”, then select the COM port where the relays will be assigned.



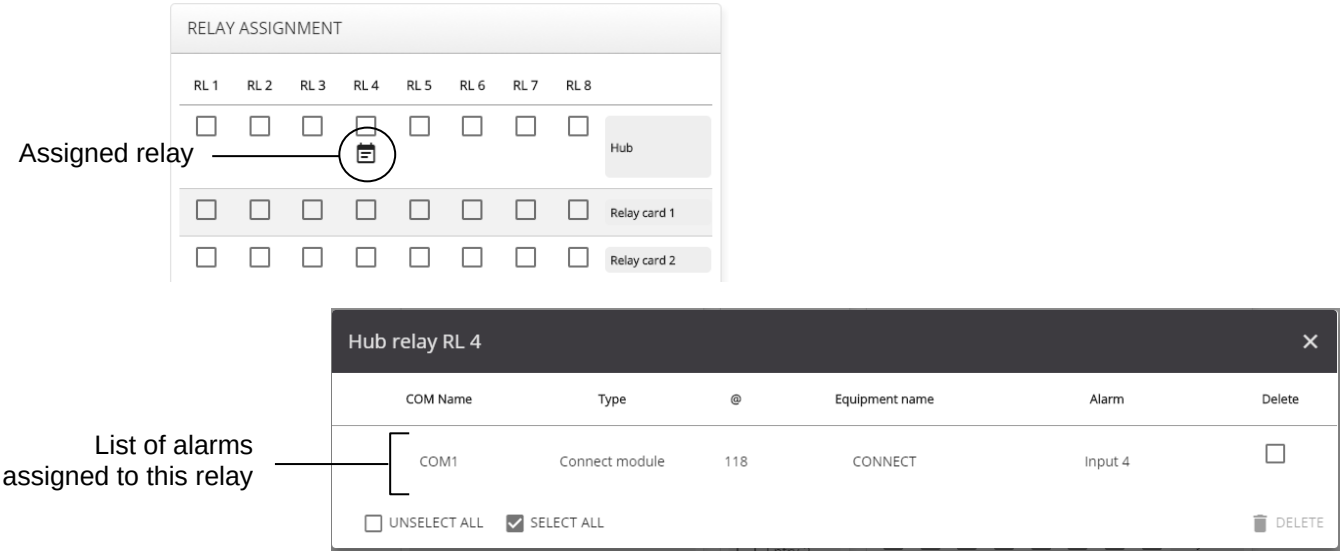
- Select equipment type.



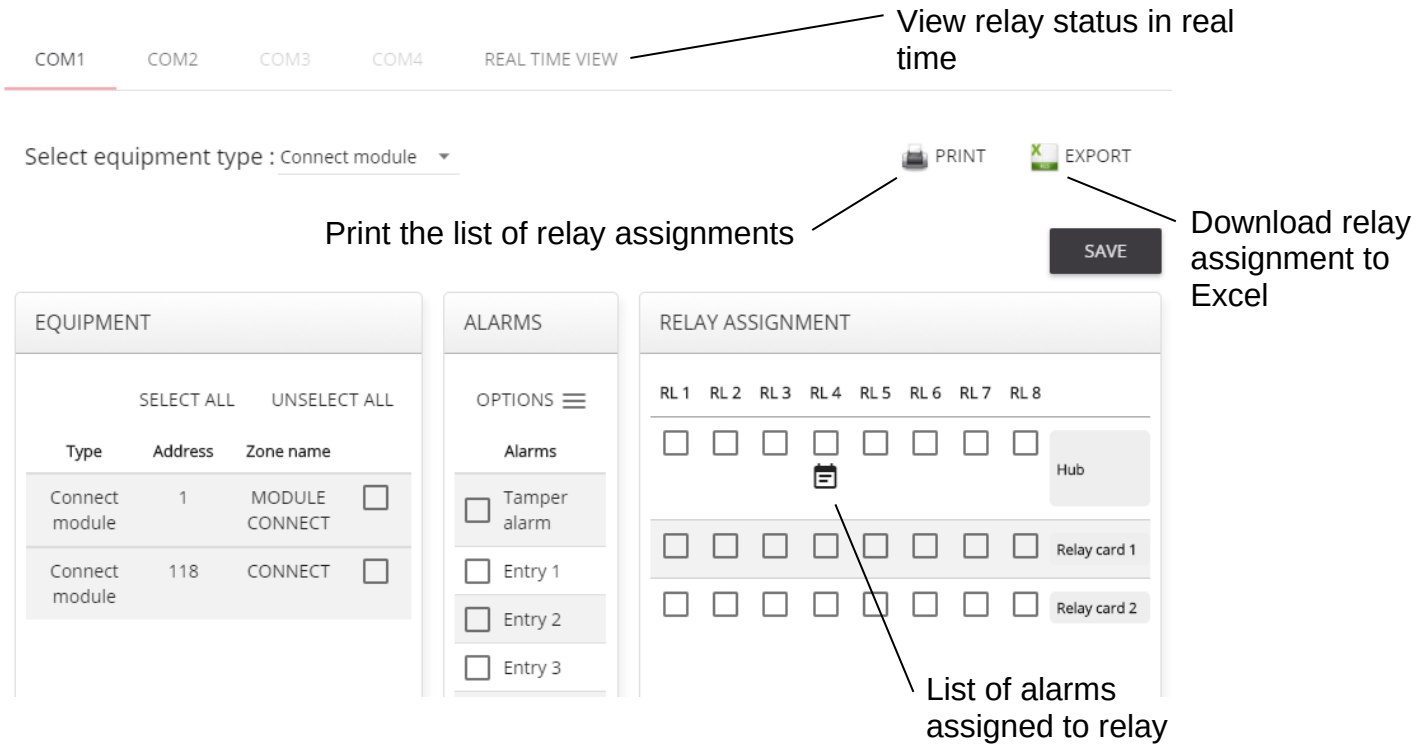
- Assign the relays:
    1. Select the equipment for which the alarms need to be assigned.
    2. Check the alarm to assign to the relays.
    3. Check the relay(s) on which the alarm will be assigned.
    4. Click “**SAVE**”.



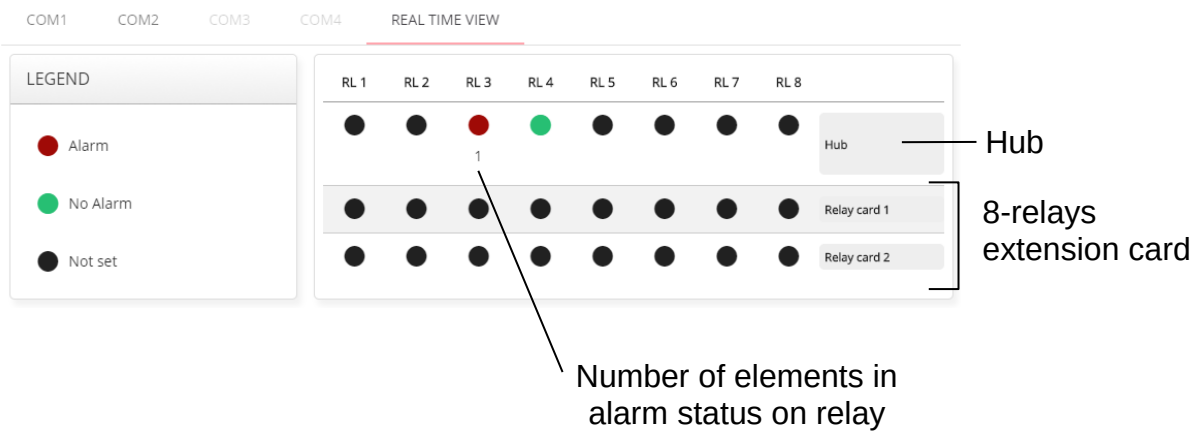
- An icon is displayed below the assigned relay.
  Click the icon to display the list of alarms assigned to this relay.



6.2 Viewing relay assignments



<u>View relay status in real time</u>:



6.3 Alarm output by MODBUS

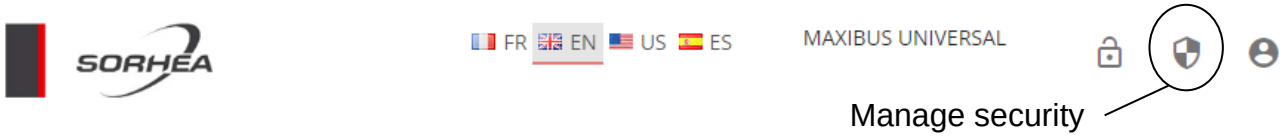
To use alarm outputs via a MODBUS link, see Communication protocol NT401.

6.4 Alarm output by API

To use alarm outputs via an API, see Communication protocol NT424.

7 ETHERNET SECURITY

To access the security management pages, click on the shield:



3 menus are available:

1. Configuration: configure HTTPS and SSH certificates
2. Certificates: manage certificates
3. 802.1X: configure network infrastructure equipment access control

7.1 Security instructions

7.1.1 Preamble

All hub installations should follow rules aimed to prevent security vulnerabilities both during configuration and in production.
It is highly recommended that such rules are followed where sensitive sites are involved.

7.1.2 HTTP or HTTPS connection

The configuration interface is accessed via a web browser.
In factory configuration and before any certificates have been installed, the hub is accessed over HTTP. Communication is not encrypted in this mode. It is therefore highly recommended to restrict its use to isolated networks to avoid the risk of data exchanges being captured. Once a certificate is installed and HTTPS is activated, access is only available over HTTPS, thus guaranteeing data exchange security.

7.1.3 SSH

You are strongly advised not to enable SSH password-protected connections as they represent a significant security vulnerability.
If they must be used, perhaps for technical support purposes, they should only be enabled on a temporary basis and should be disabled upon finishing.

7.1.4 Procedure for securing a hub for the first time

This section lists the operations to carry out in chronological order and sets out their purpose in terms of security.

1. Login to the hub over HTTP.
   Configure the module network settings: IP Address, Network Mask, etc. (see §4.3).
   This information is normally supplied by the site network administrator or RSSI (Head of Information System Security)

2. Generate, Sign and Install these certificates for HTTPS, TLS, and 802.1x as necessary
   See §7.2 Managing certificates and §7.3 802.1X for further details.
   The purpose of this stage is to secure the network exchanges when configuring the Web interface, communication with the hub, and access to enterprise network infrastructure secured using the 802.1x protocol, if applicable.

3. Login to the hub over HTTPS and change the default passwords to permanent ones or temporary ones valid for the duration of the configuration work.

7.2 Managing certificates

This page is used to:

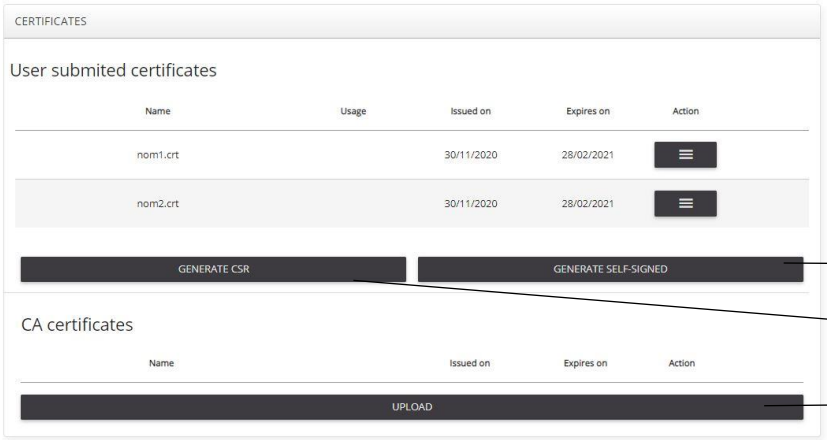
- Create self-signed certificates
- Create and export CSR or Certificate Signing Request certificates that need to be signed by a certification authority
- Import a signed certificate
- Import Trusted Root Certification Authority certificates.

These certificates will be needed for TLS communications secured with self-signed/signed certificates and for securing the web page using HTTPS.

➢ What is a certificate?

A digital (or electronic) certificate is a digital file used to secure TCP communication between different machines. The information contained in the file is used to:

- Authenticate the user to confirm that the devices are authorized to communicate with each other and thereby prevent intrusion attempts
- Provide the keys needed to encrypt communication between the devices

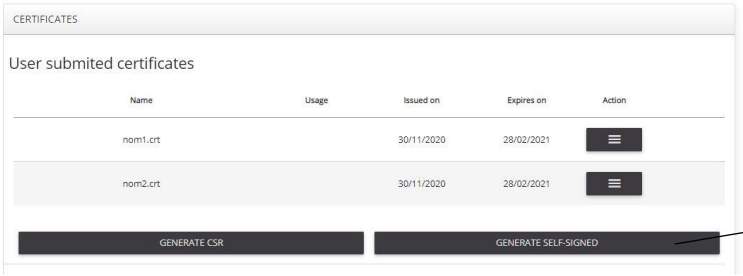


➢ Self-signed certificates

Self-signed certificates are certificates that are created and signed by the hub itself using information entered by the user.

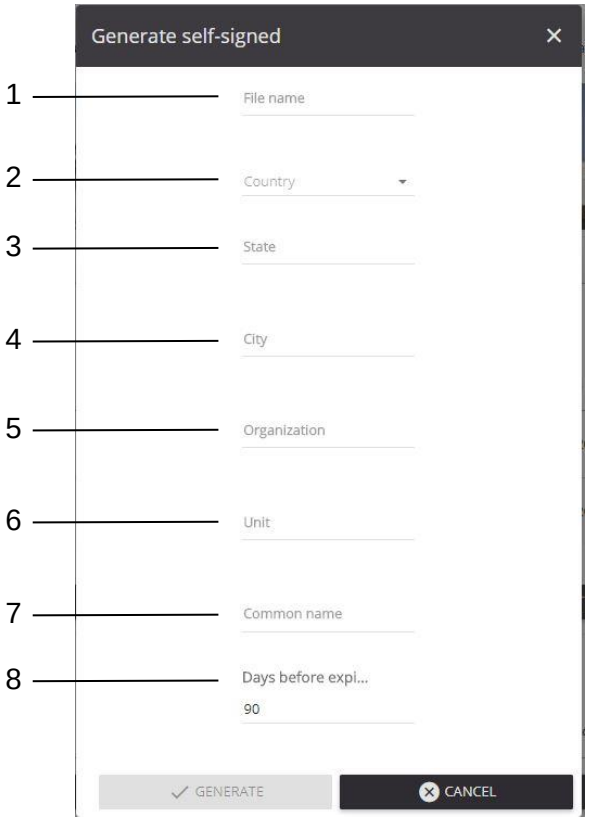
To generate this type of certificate:

1. Click on the “GENERATE SELF-SIGNED” button



Generate self-signed certificates

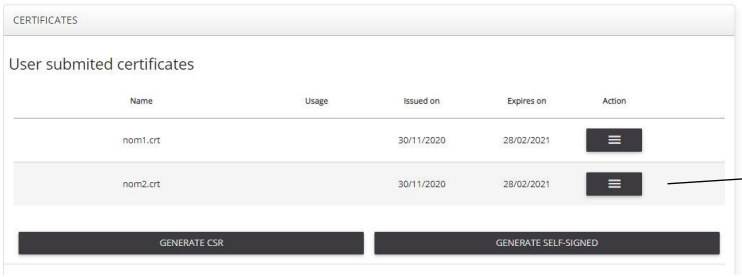
2. Fill in the required data



1- File name: name to give the generated file
2- Country: select the country
3- State: state/region/county
4- City: city
5- Organization: company
6- Unit: department
7- Common name: IP address of the hub or host name
8- Days before expiration: remaining number of days the certificate is valid

Once all the data has been validated, a row is created in the table located in the “User certificates” section. The configured filename appears in the first column and a notification that the certificate is being created appears in the last column.

3. Wait approximately 1 minute for the certificate to be generated. The certificate is ready for use when the “Generated” and “Expires” columns are populated.



The certificate is now ready for use either to secure the HTTPS web page (Configuration / Security) or to configure TCP communication security (Configuration / Network).
When the certificate is used for one or other of these two applications, the “Usage” column in the table is filled in.

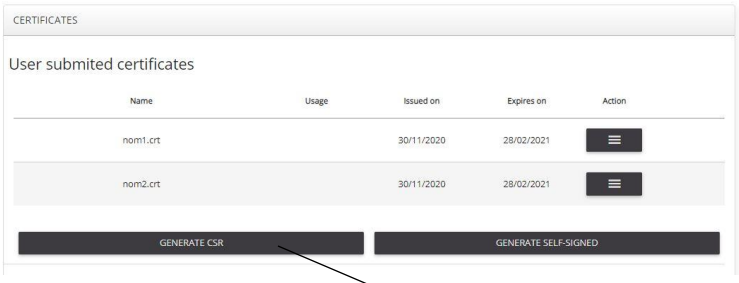
- **Signed Certificates**

Two steps are involved in configuring signed certificates:

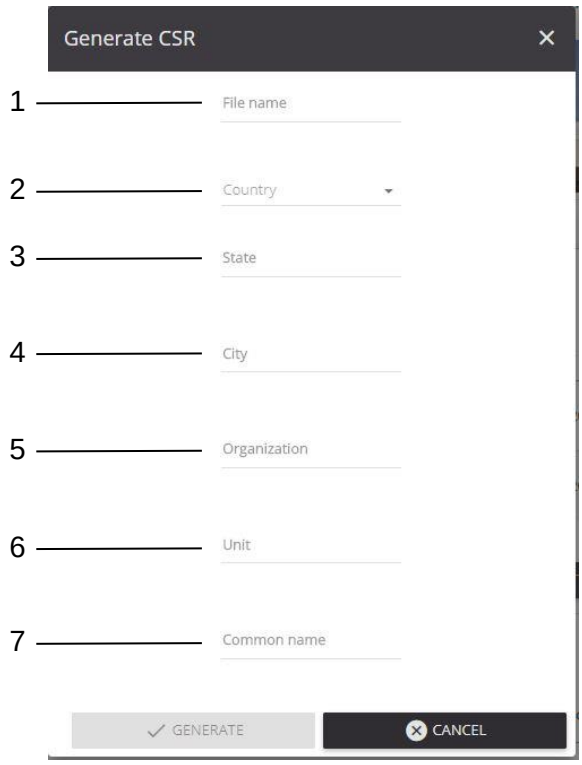
- The first step is to generate a CSR certificate (Certificate Signing Request) to be submitted to a Certification Authority for signing.
- The second step is to reimport the newly signed certificate returned by the Certification Authority.

To generate the unsigned certificate, follow the steps below:

1. Click on the “GENERATE CSR” button



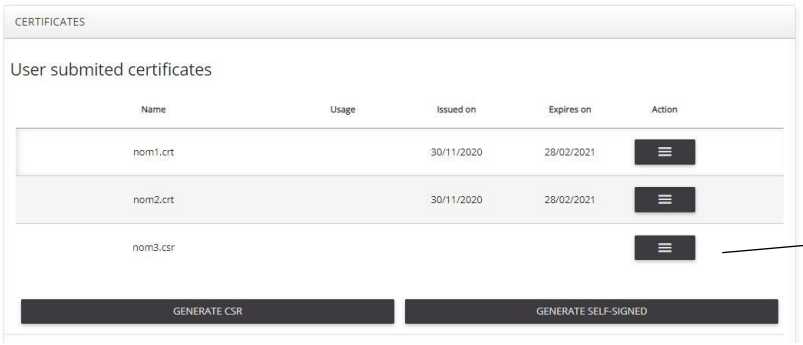
2. Fill in the required data:



1- File name: name to give the generated file
2- Country: select the country
3- State: state/region/county
4- City: city
5- Organization: company
6- Unit: department
7- Common name: IP address of the hub or host name

Once all the data has been validated, a row is created in the table located in the “User certificates” section. The configured filename appears in the first column and a notification that the certificate is being created appears in the last column.

3. Wait approximately 1 minute for the certificate to be generated. To download the certificate, click on the “Download” button.

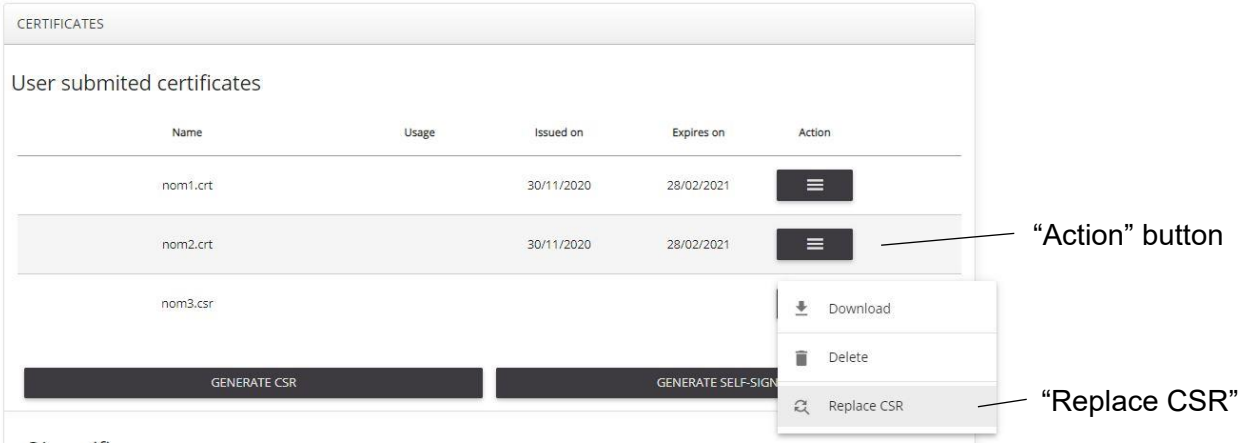


CSR certificates generated and ready

Once the CSR certificate has been generated, the file needs to be signed by a Certification Authority. This step would normally be carried out by the site’s RSSI (Head of Information System Security).

Once completed and the signed certificate returned by the RSSI, it needs to be imported:

1. Click on the “Action” button in the CSR certificate row and click on the “Replace CSR” button.



The signed certificate filename must have the same name as the CSR certificate

2. When the certificate has been imported, the “Generated” and “Expires” columns are populated.

The certificate is now ready for use either to secure the HTTPS web page (Configuration / Security) or to configure TCP communication security (Configuration / Network).

When the certificate is used for one or other of these two applications, the “Usage” column in the table is filled in.

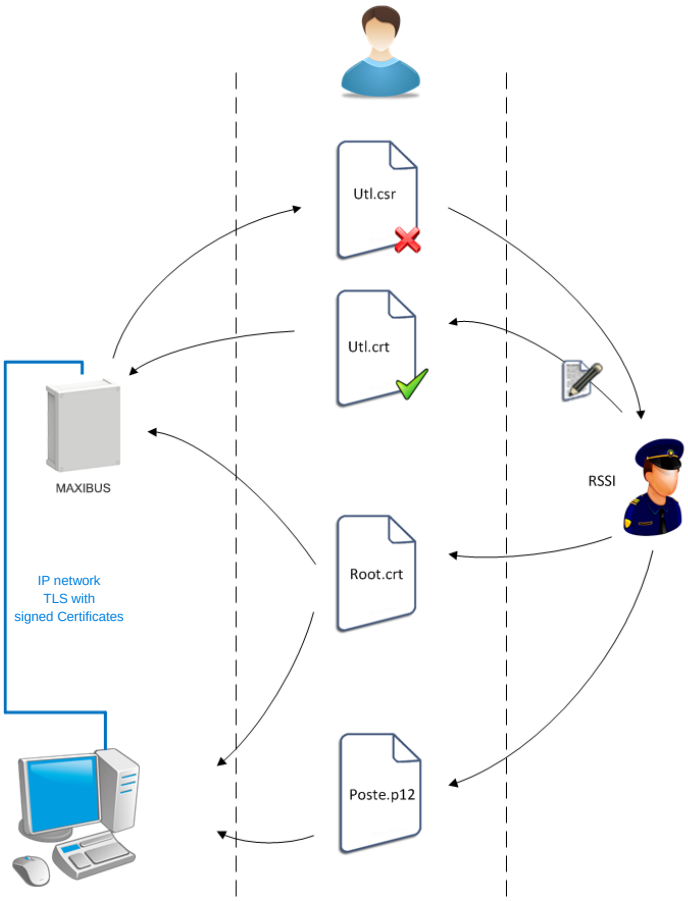
To finish configuring TLS secure communication, the root authority certificate needs to be imported into the hub. The root certificate (.crt file) is provided by the root certification authority at the same time as the signed hub certificate.

➢ CA Certificates

This section is for importing root authority certificates. Root authority certificates are provided by a root certification authority at the same time as the signed certificates. The root authority certificate needs to be imported for TLS communication to work properly.

To do so: Click on “LOAD” > Select the certificate file > Click on the “LOAD” button.

Block diagram showing how to manage certificates when using TLS communication with signed certificates:



7.3 802.1X

1. Prerequisites:

   Network infrastructure that supports 802.1X.

   If your network infrastructure does not support 802.1X, the hub will become inaccessible when you confirm the 802.1X configuration.

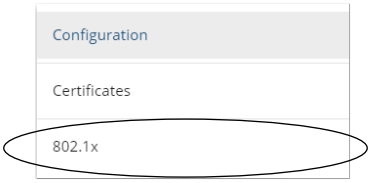
2. Modes and configuration:

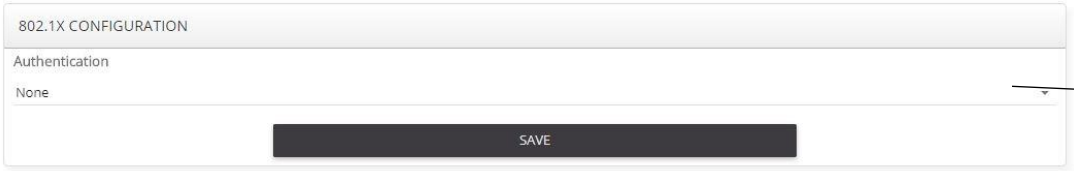
   Please contact your IT department for details on the type of authorisation used and the connection settings.

   For MD5, MSCHAPV2 and GTC authentication:
   - EAP mode (Extensible Authentication Protocol)
   - Anonymous Identity
   - CA Certificate
   - Username
   - Password

   For TLS authentication:
   - Username
   - CA Certificate
   - User Certificate

Click on the shield followed by “802.1X”:





Select the authentication mode

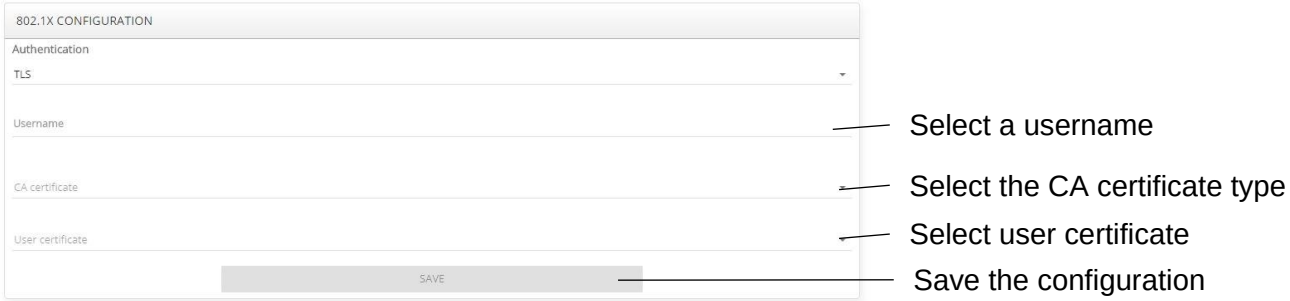
List of authentication methods:

- “MD5” mode:

- “MSCHAPV2” mode:

- “GTC” mode :

- “TLS” mode :



The following list contains the compatible EAP types and different modes of authentication:

- PEAP is an 802.1X authentication method using public key certificates on the server to authenticate clients with the server. PEAP authentication generates an encrypted TLS/SSL link between the client and the authentication server. Data exchanges are encrypted and stored in the link to ensure that the user identifiers are secured.
- EAP-GTC (Generic Token Card) is an authentication method using cleartext to exchange authentication parameters between the client and the server. This authentication method uses single use, One-Time Tokens. This is a secure identifier exchange method.

  EAP-GTC is defined in RFC 2284.
- EAP-MD5 authentication verifies an MD5 hash of the user's password.
  This authentication method is frequently used in trusted networks.

  EAP-MD5 is defined in RFC 2284.
- EAP-TLS (Transport Layer Security) is an authentication method using PKI (Public Key Infrastructure) and RADIUS server authentication, amongst others.
  It requires a client-side certificate to communicate with the authentication server.

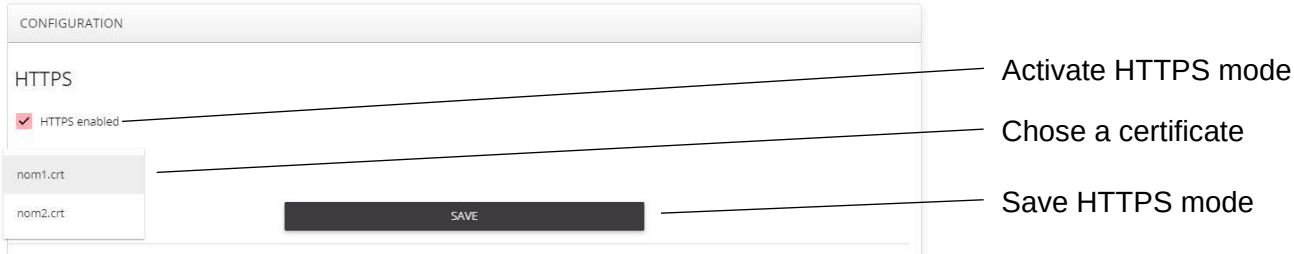
  EAP-TLS is defined in RFC 5216.
- The EAP-TTLS (Lined Transport Layer Security) method uses server-side certificates to perform the authentication between the clients and the server. Authentication does, nevertheless, rely on passwords.

  EAP-TTLS is defined in RFC 5281.
- The EAP-MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2) authentication method is used extensively in MICROSOFT systems.
  It requires a RADIUS server to be used as a backend authentication server.

  EAP-MS-CHAPv2 is defined in RFC 2759.

7.4 HTTPS

HTTPS mode is activated from the configuration menu by clicking on the shield .
To enter safe mode, tick the case "HTTPS enabled" and chose a certificate within the list of certificates owned by the concentrator (see §7.2) :



Once the certificate is selected, click on save. From now and on, the hub will redirect the current page to safe mode (https://1.2.3.4).

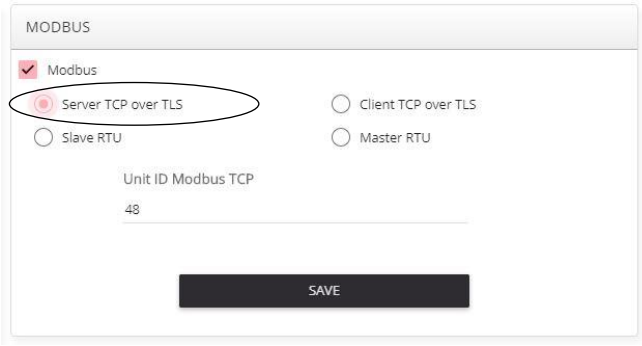
7.5 Encrypted Modbus

Securing the ModBus IP involves setting up TLS tunnels through which the ModBus data will pass. The tunnels in place use the possibility of TLS to do port forwarding by encapsulating the data in an encrypted tunnel.

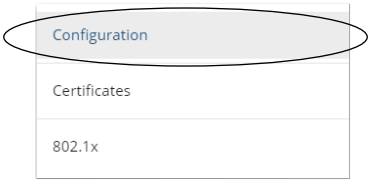
7.5.1 Encrypted Modbus Server

To be able to use the encryption, activate the TLS server of the MAXIBUS:

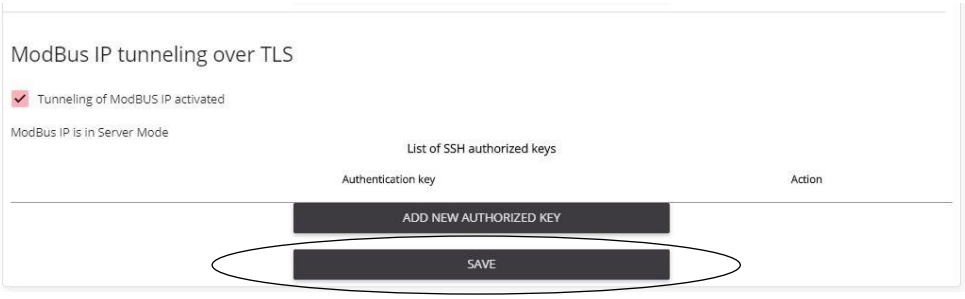
– In the "Hub" tab, Activate the Modbus Server TCP over TLS, then save.



– Click on the shield followed by “Configuration”:



– Activate "ModBus IP tunneling over TLS" then click on "Save".

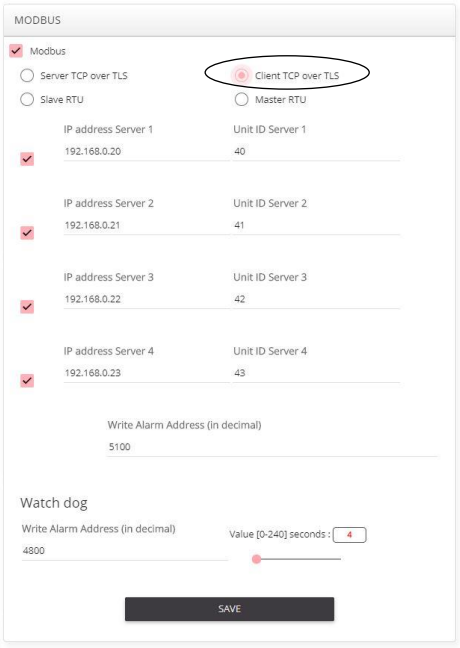


Note: If the TLS tunnel is activated to secure the ModBus, it is necessary to be able to use the mapping to activate the management of this tunnel on the client PC.
In the appendix, an example of the implementation of the encryption towards the mapping software.
(See APPENDIX: How to activate Tunneling on the client PC p.79)

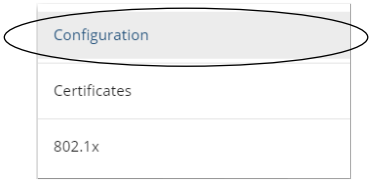
7.5.2 Encrypted Modbus Client

To encrypt the Modbus Client, follow the steps below:

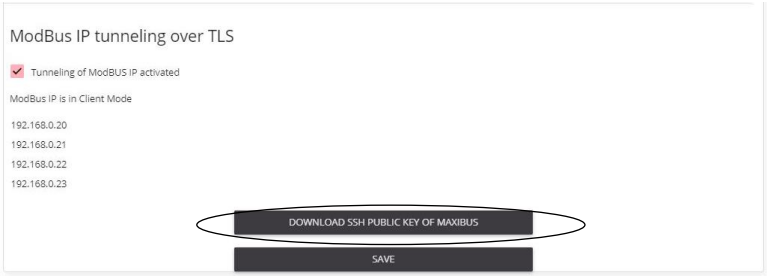
– In the "Hub" tab, Activate the Modbus Client TCP over TLS, then save.



– Click on the shield followed by “Configuration”:

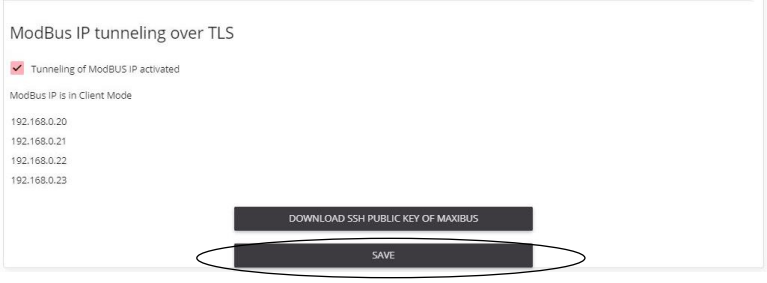


– Activate "ModBus IP tunneling over TLS" then click on "DOWNLOAD SSH PUBLIC KEY OF MAXIBUS".



The machines in front of the MAXIBUS must have a TLS server.
Place this file in the authorized TLS keys.
For example, for a Unix machine using OpenSSH, the retrieved key must be placed in the file “/home/root/.ssh/authorized_keys”.

Click on the “SAVE” button.

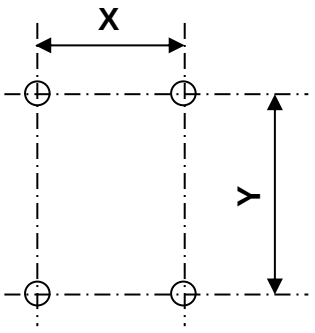


8 TECHNICAL FEATURES

MAXIBUS UNIVERSAL HUB CARD	
• Power supply	12V DC (10,5 to 14V)
• Maximum consumption alarm status off	230 mA
• 4 COM ports • Communication speed	RS485 2 wires 9600 bauds
• Link for alarms transfer • Communication speed • Communication protocol	RS485 2 wires 9600bds 1 bit start / 8 bits data / 1 bit stop MODBUS RTU
• Link for alarms transfer • Communication speed • Communication protocol	Ethernet RJ45 100 Mbits/s MODBUS TCP
• Link for maintenance and settings • Communication speed • Communication protocol	Ethernet RJ45 100 Mbits/s HTTP server
• 8 alarm outputs by NC contact alarm off	30V AC/DC – 1A
8-RELAY EXTENSION CARD	
• Power supply	12V DC (10,5 to 14V)
• Consumption	85 mA
• 8 alarm outputs by NC contact alarm off	30V AC/DC – 1A
GENERAL FEATURES OF MAXIBUS UNIVERSAL HUB	
• Operating temperature	0°C to + 55°C / 32°F to 131°F
• Protection Index	IP33
• Electromagnetic compatibility	Conforms to European standard (label **CE**)
• Maximum number of relays (maximum 16 8-relay extension cards)	136

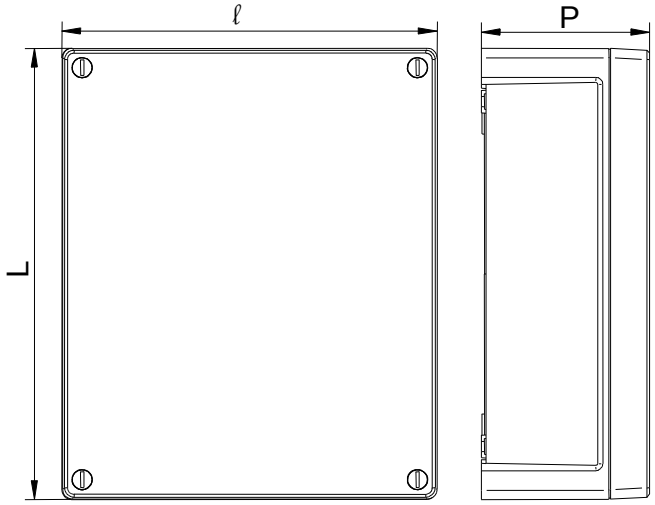
The template shows the drilling dimensions for the MAXIBUS UNIVERSAL hub with 1 to 8 extension cards and of the MAXIBUS UNIVERSAL hub with 1 to 16 extension cards:

	X	**Y**
Hub with 1 to 8 8-relay extension cards	188 mm / 7.4 in	268 mm / 10.6 in
Hub with 9 to 16 8-relay extension cards	360 mm / 14.2 in	460 mm / 18.1 in
SO-BUS HUB (1 8-relay extension card)	163.5 mm / 6.44 in	163.5 mm / 6.44 in



Dimensions:

MAXIBUS UNIVERSAL HUB



	L	ℓ	P
Hub with 1 to 8 8-relay extension cards	290 mm / 11.4 in	240 mm / 9.5 in	110 mm / 4.3 in
Hub with 9 to 16 8-relay extension cards	500 mm / 19.7 in	400 mm / 15.8 in	150 mm / 5.9 in
SO-BUS Hub (1 8-relay extension card)	180 mm / 7.09 in	180 mm / 7.09 in	100 mm / 3.94 in

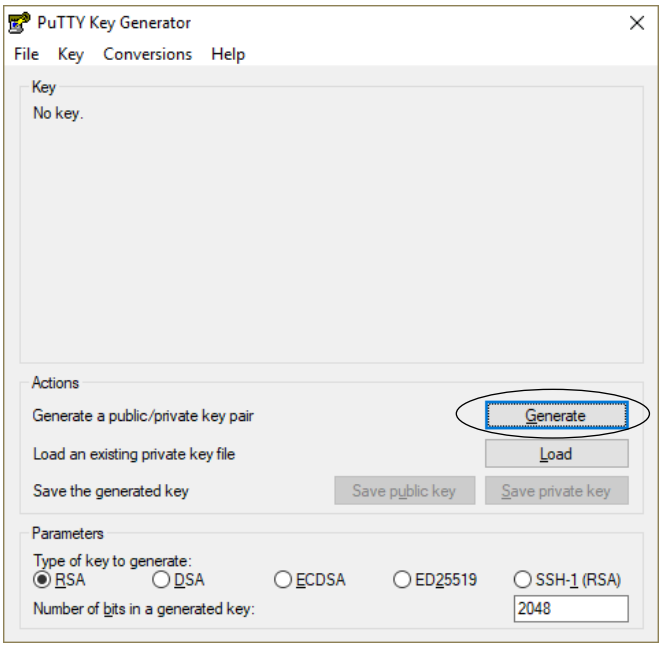
9 REFERENCES PRODUCT

- MAXIBUS UNIVERSAL hub 2 COM port with 1 to 8 8-relay extension cards ref: 30792001
- MAXIBUS UNIVERSAL hub 4 COM port with 1 to 8 8-relay extension cards ref: 30792002
- MAXIBUS UNIVERSAL hub 2 COM port with 9 to 16 8-relay extension cards ref: 30792011
- MAXIBUS UNIVERSAL hub 4 COM port with 9 to 16 8-relay extension cards ref: 30792012
- SO-BUS hub 2 COM port with 1 8-relay extension cards ref: 30825000
- 8-relay extension card ref: 35588419
- Graphic software for G-FENCE 3000 ref: 38703901
- MAXIBUS UNIVERSAL 2 COM port card ref: 80901229
- MAXIBUS UNIVERSAL 4 COM port card ref: 80901230
- 8-relay extension card kit ref: 80901218
- Empty housing hub ref: 80901231

APPENDIX: How to activate Tunneling on the client PC

- **Generation of the authentication key**

To start with, you will need to create a public/private key pair using the PuTTYgen software.

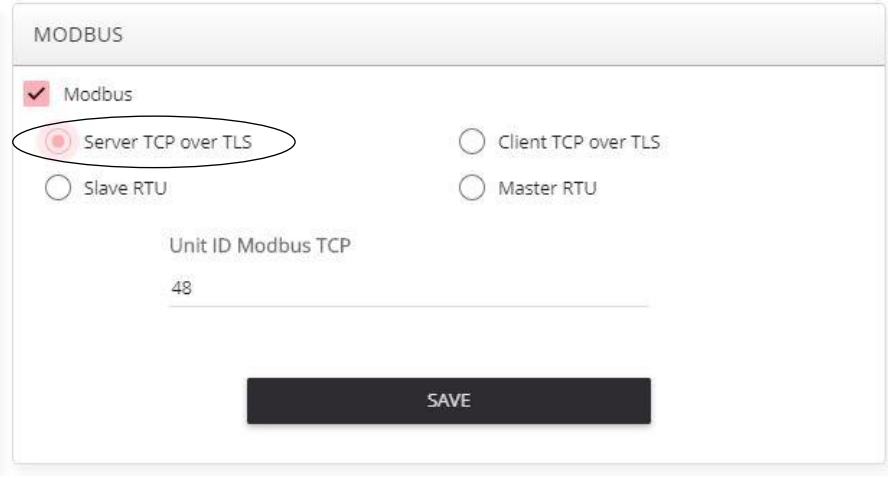


Create an RSA key pair, then save the private key by pressing the “Save private key” button.

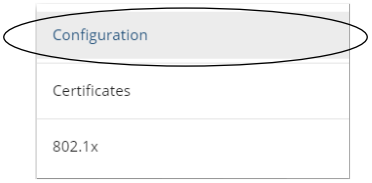
The SSH format public key is displayed in the software and should be cut and pasted into a file (not exported using the “Save public key” button).

Login to the MAXIBUS.

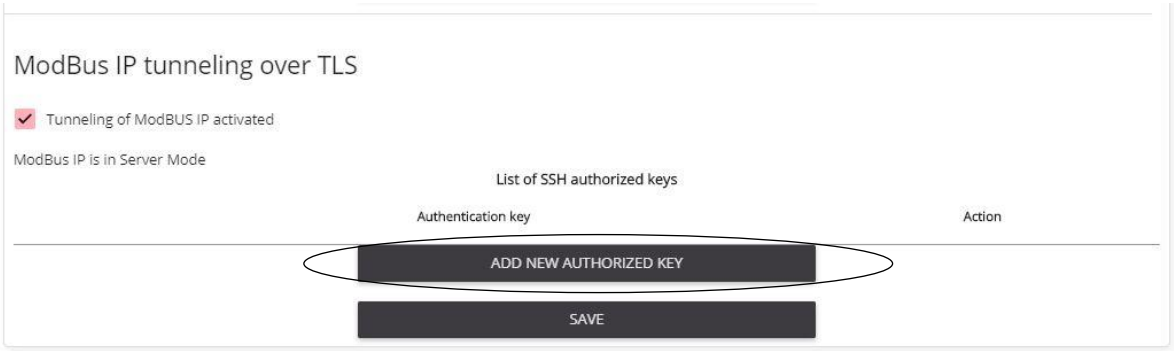
Enable the Modbus Server TCP over TLS:



– Click on the shield followed by “Configuration”:



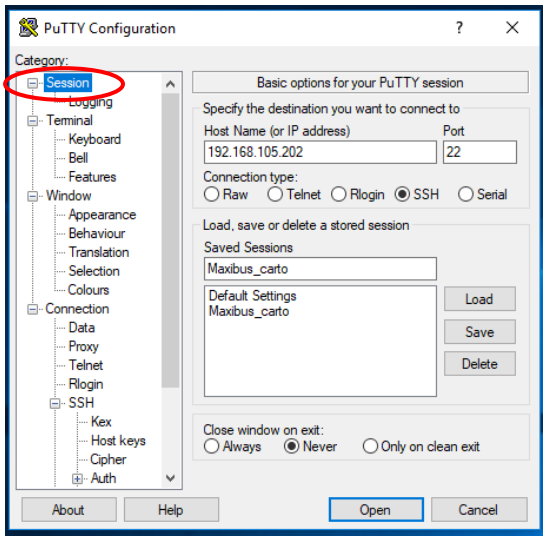
Download the file containing the public key from the MAXIBUS Web interface:



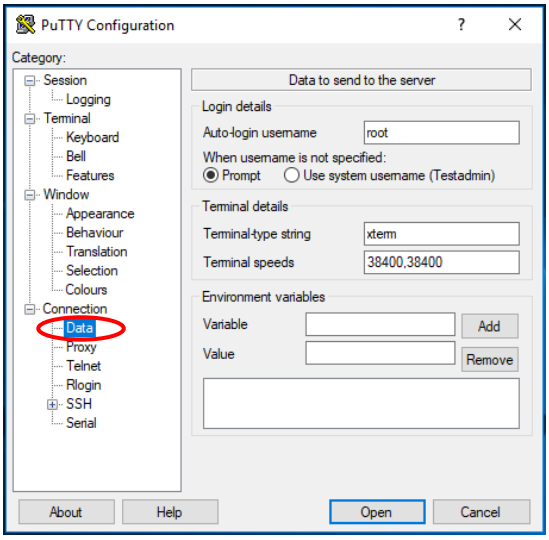
- **PuTTY configuration**

The tabs below will need configuring to produce an SSH tunnel to the MAXIBUS (IP address 192.168.105.202):

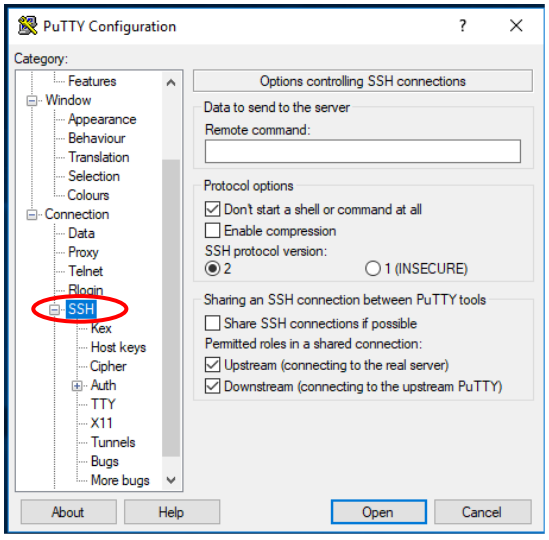
– “Session” tab



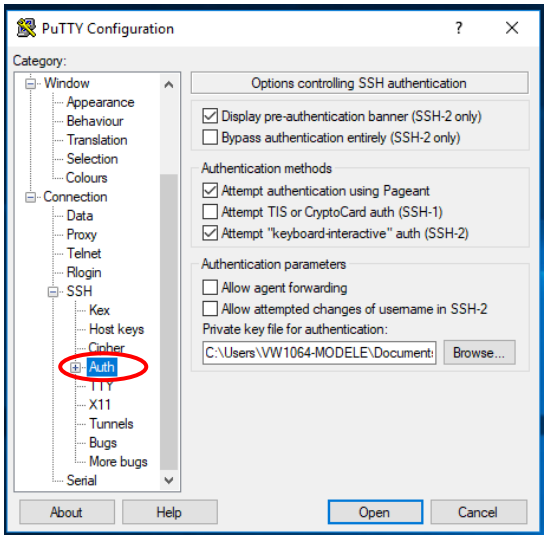
– “Connection / Data” tab



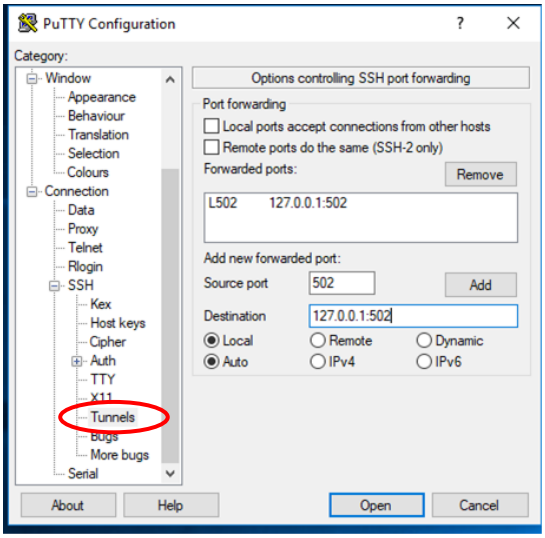
– “Connection / SSH” tab



– “Connection / SSH / Auth” tab Enter the private key you have just saved. Please note that the first 2 fields are reversed in certain versions of Putty.



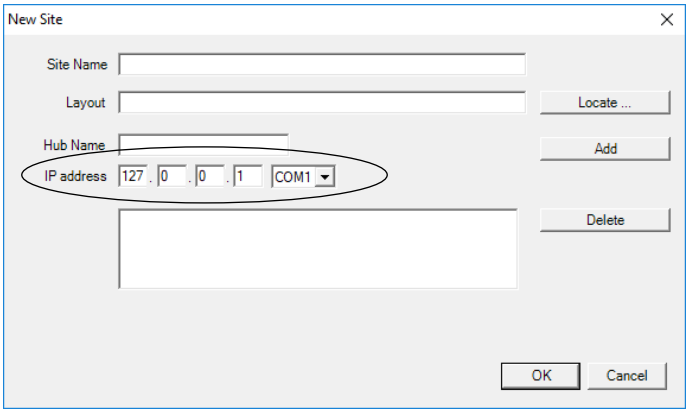
– “Connection / SSH / Tunnels” tab



– Click on “Open”
– Leave the window open.

- **Map configuration**

Set the hub address to 127.0.0.1



In compliance with the European environmental directives, this product must not be thrown away but recycled through an appropriate subsidiary.